PCT/JP2004/011303

30.07.2004

REC'D 16 SEP 2004

WIPO PCT

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

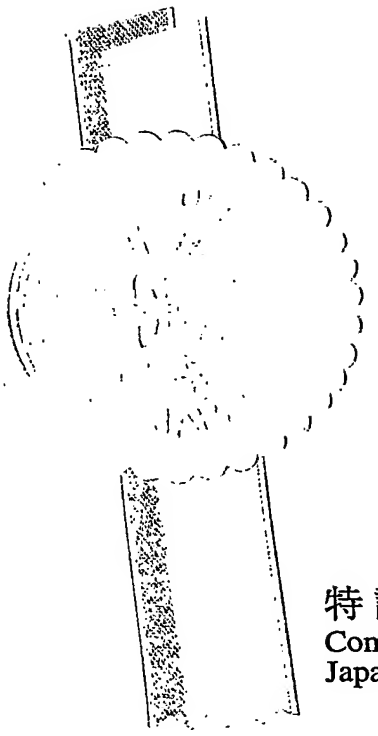
This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００３年　８月　５日

出願番号
Application Number: 特願２００３－２８６６５７

[ST. 10/C]: [ＪＰ２００３－２８６６５７]

出願人
Applicant(s): 松下電器産業株式会社



PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

２００４年　９月　３日

特許庁長官
Commissioner,
Japan Patent Office

小川洋

出証番号　出証特２００４－３０７９１２５

【書類名】　特許願
【整理番号】　2130050347
【提出日】　平成15年 8月 5日
【あて先】　特許庁長官殿
【国際特許分類】　G09C　1/00
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　山本　直紀
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　石原　秀志
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　館林　誠
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　中野　稔久
【特許出願人】
　【識別番号】　000005821
　【氏名又は名称】　松下電器産業株式会社
【代理人】
　【識別番号】　100097445
　【弁理士】
　【氏名又は名称】　岩橋　文雄
【選任した代理人】
　【識別番号】　100103355
　【弁理士】
　【氏名又は名称】　坂口　智康
【選任した代理人】
　【識別番号】　100109667
　【弁理士】
　【氏名又は名称】　内藤　浩樹
【手数料の表示】
　【予納台帳番号】　011305
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　特許請求の範囲　1
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
　【包括委任状番号】　9809938

【書類名】特許請求の範囲
【請求項１】
コンテンツを暗号化して記録する記録装置と、前記暗号化コンテンツを記録する記録媒体と、前記記録媒体に記録された前記暗号化コンテンツを読み出して復号する再生装置とからなる著作権保護システムであって、
前記再生装置はＮ個（Ｎは２以上の自然数）のカテゴリに分類されており、
前記記録装置は、メディア鍵と前記Ｎ個の各カテゴリに属する再生装置が保有するデバイス鍵データとから前記各カテゴリの特定の再生装置が保有するデバイス鍵を無効化するための無効化データを前記Ｎ個の各カテゴリに対してそれぞれ生成し、前記メディア鍵に基づいて前記コンテンツを暗号化した暗号化コンテンツを生成し、前記Ｎ個の無効化データと前記暗号化コンテンツを前記記録媒体に記録し、
前記再生装置は、前記記録媒体から前記Ｎ個の無効化データのうち、前記再生装置が属するカテゴリ用の無効化データ及び前記暗号化コンテンツを読み出し、読み出した前記無効化データに基づいて前記暗号化コンテンツを復号することを特徴とする著作権保護システム。
【請求項２】
前記Ｎ個の各無効化データは、対応するカテゴリの再生装置が保有するデバイス鍵データで前記メディア鍵を暗号化した暗号化メディア鍵データであり、
前記各カテゴリの再生装置は、前記記録媒体から対応する前記暗号化メディア鍵データ及び前記暗号化コンテンツを読み出し、保有するデバイス鍵で前記暗号化メディア鍵データを復号して前記メディア鍵を取得し、取得した前記メディア鍵に基づいて前記暗号化コンテンツを復号しすることを特徴とする請求項１記載の著作権保護システム。
【請求項３】
前記記録装置は、前記メディア鍵に基づいて暗号化鍵を生成し、前記暗号化鍵に基づいて前記コンテンツを暗号化し、
前記各カテゴリの再生装置は、取得した前記メディア鍵に基づいて復号鍵を生成し、生成した前記復号鍵に基づいて前記暗号化コンテンツを復号することを特徴とする請求項２記載の著作権保護システム。
【請求項４】
前記記録装置は、コンテンツ鍵で前記コンテンツを暗号化し、前記メディア鍵で前記コンテンツ鍵を暗号化して暗号化コンテンツ鍵を生成し、生成した前記暗号化コンテンツ鍵を前記記録媒体に記録し、
前記各カテゴリの再生装置は、前記記録媒体から前記暗号化コンテンツ鍵を読み出し、前記メディア鍵で前記暗号化コンテンツ鍵を復号してコンテンツ鍵を取得し、取得した前記コンテンツ鍵で前記暗号化コンテンツを復号することを特徴とする請求項２記載の著作権保護システム。
【請求項５】
前記Ｎ個の各無効化データは対応するカテゴリの再生装置が保有するデバイス鍵データで前記対応するカテゴリ用のメディア鍵を暗号化した暗号化メディア鍵データであり、
前記記録装置は、コンテンツ鍵で前記コンテンツを暗号化し、前記コンテンツ鍵を前記Ｎ個のメディア鍵で暗号化してＮ個の暗号化コンテンツ鍵を生成し、前記Ｎ個の暗号化メディア鍵データと前記Ｎ個の暗号化コンテンツ鍵と前記暗号化コンテンツを記録媒体に記録し、
前記各カテゴリの再生装置は、前記記録媒体から対応するカテゴリ用の暗号化メディア鍵データと対応するカテゴリ用の暗号化コンテンツ鍵と前記暗号化コンテンツとを読み出し、保有するデバイス鍵で前記暗号化メディア鍵データを復号して前記対応するカテゴリ用のメディア鍵を取得し、取得した前記対応するカテゴリ用のメディア鍵で前記対応するカテゴリ用の暗号化コンテンツ鍵を復号して前記コンテンツ鍵を取得し、取得した前記コンテンツ鍵で前記暗号化コンテンツを復号することを特徴とする請求項１記載の著作権保護システム。

【請求項６】
コンテンツに暗号化処理を施して記録する記録装置と、前記暗号化コンテンツを記録する記録媒体と、前記記録媒体に記録された前記暗号化コンテンツを読み出して復号する第２のカテゴリの再生装置と、前記記録媒体に記録された前記暗号化コンテンツを読み出して複合処理の一部を行う前記第２のカテゴリの読み出し装置及び前記第２のカテゴリの読み出し装置に接続され前記暗号化コンテンツの複合処理の一部を行う第１のカテゴリの復号装置とから構成される再生装置とからなる著作権保護システムであって、
前記記録装置は、メディア鍵と前記第１のカテゴリの復号装置が保有するデバイス鍵データとから前記第１のカテゴリの特定の復号装置が保有するデバイス鍵を無効化するための第１の無効化データを生成し、前記メディア鍵と前記第２のカテゴリの装置が保有するデバイス鍵データとから前記第２のカテゴリの特定の装置が保有するデバイス鍵を無効化するための第２の無効化データを生成し、前記メディア鍵に基づいて前記コンテンツに暗号化処理を施した暗号化コンテンツを生成し、前記第１の無効化データ、前記第２の無効化データ及び前記暗号化コンテンツを前記記録媒体に記録し、
前記第２のカテゴリの再生装置は、前記記録媒体から前記第２の無効化データ及び前記暗号化コンテンツを読み出し、前記第２の無効化データに基づいて前記暗号化コンテンツを復号し、
前記第２のカテゴリの読み出し装置は、前記記録媒体から前記第１の無効化データ、前記第２の無効化データ及び前記暗号化コンテンツを読み出し、前記第２の無効化データに基づいて前記暗号化コンテンツの復号処理の一部を施した中間データ及び前記第１の無効化データを前記第１カテゴリの復号装置に供給し、
前記第１のカテゴリの復号装置は、前記第２のカテゴリの読み出し装置から供給される前記中間データに前記第１の無効化データに基づいて復号処理を施し前記コンテンツを取得することを特徴とする著作権保護システム。
【請求項７】
コンテンツを暗号化して記録する記録装置であって、
前記記録装置は、メディア鍵とＮ個（Ｎは２以上の自然数）のカテゴリに分類された各カテゴリに属する再生装置が保有するデバイス鍵データとから前記各カテゴリの特定の再生装置が保有するデバイス鍵を無効化するための無効化データを前記Ｎ個の各カテゴリに対してそれぞれ生成し、前記メディア鍵に基づいて前記コンテンツを暗号化した暗号化コンテンツを生成し、前記Ｎ個の無効化データと前記暗号化コンテンツを前記記録媒体に記録することを特徴とする記録装置。
【請求項８】
前記Ｎ個の各無効化データは対応するカテゴリの再生装置が保有するデバイス鍵データで前記メディア鍵を暗号化した暗号化メディア鍵データであることを特徴とする請求項７記載の記録装置。
【請求項９】
前記記録装置は、前記メディア鍵に基づいて暗号化鍵を生成し、前記暗号化鍵に基づいて前記コンテンツを暗号化することを特徴とする請求項８記載の記録装置。
【請求項１０】
前記記録装置は、コンテンツ鍵で前記コンテンツを暗号化し、前記メディア鍵で前記コンテンツ鍵を暗号化した暗号化コンテンツ鍵を生成し、生成した前記暗号化コンテンツ鍵を前記記録媒体に記録することを特徴とする請求項８記載の記録装置。
【請求項１１】
前記Ｎ個の各無効化データは、対応するカテゴリの再生装置が保有するデバイス鍵データで前記対応するカテゴリ用のメディア鍵を暗号化した暗号化メディア鍵データであり、
前記記録装置は、コンテンツ鍵で前記コンテンツを暗号化し、前記コンテンツ鍵を前記Ｎ個のメディア鍵で暗号化してＮ個の暗号化コンテンツ鍵データを生成し、前記Ｎ個の暗号化メディア鍵データと前記Ｎ個の暗号化コンテンツ鍵と前記暗号化コンテンツを記録媒体に記録することを特徴とする請求項７記載の記録装置。

【請求項１２】
コンテンツを暗号化して記録する記録装置であって、
　前記記録装置は、メディア鍵と第１のカテゴリの復号装置が保有するデバイス鍵データとから前記第１のカテゴリの特定の復号装置が保有するデバイス鍵を無効化するための第１の無効化データを生成し、前記メディア鍵と前記第２のカテゴリの装置が保有するデバイス鍵データとから前記第２のカテゴリの特定の装置が保有するデバイス鍵を無効化するための第２の無効化データを生成し、前記メディア鍵に基づいて前記コンテンツに暗号化処理を施した暗号化コンテンツを生成し、前記第１の無効化データ、前記第２の無効化データ及び前記暗号化コンテンツを前記記録媒体に記録することを特徴とする記録装置。
【請求項１３】
暗号化コンテンツを記録する記録媒体であって、
　前記記録媒体は、メディア鍵とＮ個（Ｎは２以上の自然数）のカテゴリに分類された各カテゴリの再生装置が保有するデバイス鍵データとから生成された前記各カテゴリの特定の再生装置が保有するデバイス鍵を無効化するための無効化データと、前記メディア鍵に基づいてコンテンツを暗号化して生成された暗号化コンテンツを記録することを特徴とする記録媒体。
【請求項１４】
前記Ｎ個の無効化データは、対応するカテゴリの再生装置が保有するデバイス鍵データで前記メディア鍵を暗号化した暗号化メディア鍵データであることを特徴とする請求項１３記載の記録媒体。
【請求項１５】
前記暗号化コンテンツは、前記メディア鍵に基づいて生成された暗号化鍵に基づいて前記コンテンツを暗号化して生成されたものであることを特徴とする請求項１４記載の記録媒体。
【請求項１６】
前記暗号化コンテンツはコンテンツ鍵で前記コンテンツを暗号化して生成されたものであり、
　前記メディア鍵で前記コンテンツ鍵を暗号化して生成された暗号化コンテンツ鍵を記録することを特徴とする請求項１４記載の記録媒体。
【請求項１７】
前記Ｎ個の各無効化データは、対応するカテゴリの再生装置が保有するデバイス鍵データで前記対応するカテゴリ用のメディア鍵を暗号化した暗号化メディア鍵データであり、
　前記暗号化コンテンツは、コンテンツ鍵で前記コンテンツを暗号化して生成されたものであり、
　前記記録媒体は、前記コンテンツ鍵を前記Ｎ個のメディア鍵で暗号化して生成されたＮ個の暗号化コンテンツ鍵を記録することを特徴とする請求項１３記載の記録媒体。
【請求項１８】
暗号化コンテンツを記録する記録媒体であって、
　メディア鍵と第１のカテゴリの復号装置が保有するデバイス鍵データとから生成された前記第１のカテゴリの特定の復号装置が保有するデバイス鍵を無効化するための第１の無効化データと、前記メディア鍵と第２のカテゴリの装置が保有するデバイス鍵データとから生成された前記第２のカテゴリの特定の装置が保有するデバイス鍵を無効化するための第２の無効化データと、前記メディア鍵に基づいて前記コンテンツに暗号化処理を施して生成された暗号化コンテンツとを記録することを特徴とする記録媒体。
【請求項１９】
記録媒体に記録された暗号化コンテンツを再生する再生装置であって、
　前記再生装置はＮ個（Ｎは２以上の自然数）のカテゴリに分類されており、
　前記記録媒体には、メディア鍵と前記Ｎ個の各カテゴリの再生装置が保有するデバイス鍵データとから生成された前記各カテゴリの特定の再生装置が保有するデバイス鍵を無効化するための無効化データと、前記メディア鍵に基づいてコンテンツを暗号化して生成さ

れた暗号化コンテンツとが記録されており、
　前記再生装置は、前記記録媒体から前記Ｎ個の無効化データのうち前記再生装置が属するカテゴリ用の無効化データ及び前記暗号化コンテンツを読み出し、読み出した前記無効化データに基づいて前記暗号化コンテンツを復号することを特徴とする再生装置。
【請求項２０】
前記Ｎ個の各無効化データは、対応するカテゴリの再生装置が保有するデバイス鍵データで前記メディア鍵を暗号化した暗号化メディア鍵データであり、
　前記再生装置は、前記記録媒体から対応する前記暗号化メディア鍵データ及び前記暗号化コンテンツを読み出し、保有するデバイス鍵で前記暗号化メディア鍵データを復号して前記メディア鍵を取得し、取得した前記メディア鍵に基づいて前記暗号化コンテンツを復号することを特徴とする請求項１９記載の再生装置。
【請求項２１】
前記暗号化コンテンツは、前記メディア鍵に基づいて生成された暗号化鍵に基づいて前記コンテンツを暗号化して生成されたものであり、
　前記再生装置は、取得した前記メディア鍵に基づいて復号鍵を生成し、生成した前記復号鍵に基づいて前記暗号化コンテンツを復号することを特徴とする請求項２０記載の再生装置。
【請求項２２】
前記暗号化コンテンツは、コンテンツ鍵で前記コンテンツを暗号化して生成されたものであり、
　前記記録媒体には、前記メディア鍵で前記コンテンツ鍵を暗号化して生成された暗号化コンテンツ鍵が記録されており、
　前記再生装置は、前記記録媒体から前記暗号化コンテンツ鍵を読み出し、前記メディア鍵で前記暗号化コンテンツ鍵を復号してコンテンツ鍵を取得し、取得した前記コンテンツ鍵で前記暗号化コンテンツを復号することを特徴とする請求項２０記載の再生装置。
【請求項２３】
前記Ｎ個の無効化データは、対応するカテゴリの再生装置が保有するデバイス鍵データで前記対応するカテゴリ用のメディア鍵を暗号化した暗号化メディア鍵データであり、
　前記暗号化コンテンツは、コンテンツ鍵で前記コンテンツを暗号化して生成されたものであり、
　前記記録媒体には、前記コンテンツ鍵を前記Ｎ個のメディア鍵で暗号化して生成されたＮ個の暗号化コンテンツ鍵が記録されており、
　前記再生装置は、前記記録媒体から対応するカテゴリ用の暗号化メディア鍵データと対応するカテゴリ用の暗号化コンテンツ鍵と前記暗号化コンテンツとを読み出し、保有するデバイス鍵で前記暗号化メディア鍵データを復号して前記対応するカテゴリ用のメディア鍵を取得し、取得した前記対応するカテゴリ用のメディア鍵で前記暗号化コンテンツ鍵を復号して前記コンテンツ鍵を取得し、取得した前記コンテンツ鍵で前記暗号化コンテンツを復号することを特徴とする請求項１９記載の再生装置。
【請求項２４】
記録媒体に記録された暗号化コンテンツを再生する再生装置であって、
　前記記録媒体には、メディア鍵と第１のカテゴリの復号装置が保有するデバイス鍵データとから生成された前記第１のカテゴリの特定の復号装置が保有するデバイス鍵を無効化するための第１の無効化データと、前記メディア鍵と第２のカテゴリの装置が保有するデバイス鍵データとから生成された前記第２のカテゴリの特定の装置が保有するデバイス鍵を無効化するための第２の無効化データと、前記メディア鍵に基づいて暗号化処理を施して生成された暗号化コンテンツとが記録されており、
　前記再生装置は、前記第２のカテゴリに属し、前記記録媒体から前記第２の無効化データ及び前記暗号化コンテンツを読み出し、前記第２の無効化データに基づいて前記暗号化コンテンツを復号することを特徴とする再生装置。
【請求項２５】

記録媒体に記録された暗号化コンテンツを再生する再生装置を構成する読み出し装置であって、

前記記録媒体には、メディア鍵と第１のカテゴリの復号装置が保有するデバイス鍵データとから生成された前記第１のカテゴリの特定の復号装置が保有するデバイス鍵を無効化するための第１の無効化データと、前記メディア鍵と第２のカテゴリの装置が保有するデバイス鍵データとから生成された前記第２のカテゴリの特定の装置が保有するデバイス鍵を無効化するための第２の無効化データと、前記メディア鍵に基づいて暗号化処理を施して生成された暗号化コンテンツとが記録されており、

前記読み出し装置は、前記第２のカテゴリに属し、前記記録媒体から前記第１の無効化データ、前記第２の無効化データ及び前記暗号化コンテンツを読み出し、前記第２の無効化データに基づいて前記暗号化コンテンツの復号処理の一部を施した中間データを生成し、生成した前記中間データ及び前記第１の無効化データを出力することを特徴とする読み出し装置。

【請求項２６】

記録媒体に記録された暗号化コンテンツを再生する再生装置を構成する復号装置であって、

前記記録媒体には、メディア鍵と第１のカテゴリの復号装置が保有するデバイス鍵データとから生成された前記第１のカテゴリの特定の復号装置が保有するデバイス鍵を無効化するための第１の無効化データと、前記メディア鍵と第２のカテゴリの装置が保有するデバイス鍵データとから生成された前記第２のカテゴリの特定の装置が保有するデバイス鍵を無効化するための第２の無効化データと、前記メディア鍵に基づいて暗号化処理を施して生成された暗号化コンテンツとが記録されており、

前記第２のカテゴリの読み出し装置は、前記記録媒体から前記第１の無効化データ、前記第２の無効化データ及び前記暗号化コンテンツを読み出し、前記第２の無効化データに基づいて前記暗号化コンテンツの復号処理の一部を施した中間データを生成し、生成した前記中間データ及び前記第１の無効化データを出力し、

前記復号装置は、前記第１のカテゴリに属し、前記第２のカテゴリの読み出し装置から供給される前記中間データに前記第１の無効化データに基づいて復号処理を施して前記コンテンツを取得することを特徴とする復号装置。

【請求項２７】

記録媒体に記録された暗号化コンテンツを再生する再生装置であって、

請求項２５記載の読み取り装置と請求項２６記載の復号装置とから構成されることを特徴とする再生装置。

【請求項２８】

コンテンツを暗号化及び復号するために必要な無効化データを生成して記録する鍵生成装置と、コンテンツを暗号化して記録する記録装置と、前記無効化データと前記暗号化コンテンツを記録する記録媒体と、前記記録媒体に記録された前記暗号化コンテンツを読み出して復号する再生装置とからなる著作権保護システムであって、

前記記録装置及び前記再生装置はＮ個（Ｎは２以上の自然数）のカテゴリに分類されており、

前記鍵生成装置は、メディア鍵と前記各カテゴリに属する記録装置もしくは再生装置が保有するデバイス鍵データとから前記各カテゴリの特定の記録装置もしくは再生装置が保有するデバイス鍵を無効化するための無効化データを、前記Ｎ個の各カテゴリに対してそれぞれ生成し、生成した前記Ｎ個の無効化データを前記記録媒体に記録し、

前記記録装置は、前記記録媒体から前記Ｎ個の無効化データのうち、前記記録装置が属するカテゴリ用の無効化データを読み出し、読み出した前記無効化データに基づいてコンテンツを暗号化して暗号化コンテンツを生成し、生成した前記暗号化コンテンツを前記記録媒体に記録し、

前記再生装置は、前記記録媒体から前記Ｎ個の無効化データのうち、前記再生装置が属するカテゴリ用の無効化データ及び前記暗号化コンテンツを読み出し、読み出した前記無

効化データに基づいて前記暗号化コンテンツを復号することを特徴とする著作権保護システム。

【請求項２９】

メディア鍵とＮ個（Ｎは２以上の自然数）のカテゴリに分類された各カテゴリに属する記録装置もしくは再生装置が保有するデバイス鍵データとから前記各カテゴリの特定の記録装置もしくは再生装置が保有するデバイス鍵を無効化するための無効化データを、前記Ｎ個の各カテゴリに対してそれぞれ生成し、生成した前記Ｎ個の無効化データを前記記録媒体に記録することを特徴とする鍵生成装置。

【請求項３０】

コンテンツを暗号化して記録する記録装置であって、

メディア鍵とＮ個（Ｎは２以上の自然数）のカテゴリに分類された各カテゴリに属する記録装置もしくは再生装置が保有するデバイス鍵データとから生成された前記各カテゴリの特定の記録装置もしくは再生装置が保有するデバイス鍵を無効化するための無効化データが記録された記録媒体から、前記Ｎ個の無効化データのうち前記記録装置が属するカテゴリ用の無効化データを読み出し、

読み出した前記無効化データに基づいてコンテンツを暗号化して暗号化コンテンツを生成し、

生成した前記暗号化コンテンツを前記記録媒体に記録することを特徴とする記録装置。

【書類名】明細書
【発明の名称】著作権保護システム、鍵生成装置、記録装置、再生装置、読み出し装置、復号装置、及び記録媒体
【技術分野】
【０００１】
本発明は、映画や音楽などの著作物をデジタル化したコンテンツを、光ディスク等の大容量記録媒体に記録して、再生するシステムに関し、特にコンテンツの著作者の許可なく不正利用されることを防止する著作権保護システムに関する。
【背景技術】
【０００２】
近年、記録媒体が大容量化するに従い、映画や音楽などの著作物をデジタル化したコンテンツを例えば光ディスク等の記録媒体に格納して市販するビジネスが盛んに行われている。
【０００３】
記録媒体に記録されたコンテンツは、不正にコピーされる可能性があるため、何らかの保護が必要である。
【０００４】
一般的に、コンテンツの著作権を保護するため、即ちコンテンツの不正再生や不正コピー等といった不正利用を防止するために暗号化技術が用いられる。
【０００５】
具体的には、コンテンツをある暗号化鍵を用いて暗号化して光ディスク等の記録媒体に記録して配布する。これに対して、その暗号鍵に対応する復号鍵を保有する端末のみが、記録媒体から読み出したデータをその復号鍵を用いて復号し、コンテンツの再生等を行うことができる。
【０００６】
なお、コンテンツを暗号化して記録媒体に記録する方法としては、端末が保有する復号鍵に対応する暗号化鍵でコンテンツそのものを暗号化して記録する方法や、コンテンツをある鍵で暗号化して記録した上で、その鍵に対応する復号用の鍵を、端末が保有する復号鍵に対応する暗号化鍵で暗号化して記録する方法とがある。
【０００７】
このとき、端末が保有する復号鍵は外部に露見しないように厳重に管理される必要があるが、不正者による端末内部の解析によって、ある鍵が外部に暴露される危険性がある。ある鍵が一旦不正者に暴露されてしまうと、コンテンツを不正利用する再生装置あるいはソフトウェアを作成し、インターネット等によりそれらを流布することが考えられる。このような場合、著作権者は一旦暴露された鍵では、次から提供するコンテンツを扱えないようにしたいと考える。これを実現する技術を鍵無効化技術と呼び、鍵無効化を実現するシステムとして、特許文献１が開示されている。
【０００８】
一方、記録媒体に記録された暗号化コンテンツを再生する装置としては、記録媒体から暗号化コンテンツを読み出す機能と読み出した暗号化コンテンツを復号する機能が一体となったいわゆる民生用プレーヤや、パソコンに接続もしくは内蔵された光ディスクドライブで記録媒体から暗号化コンテンツを読み出し、読み出した暗号化コンテンツをパソコンのホスト上で動作するアプリケーションプログラムによって復号して再生するものがある。これら２つの種類の再生装置に対応する著作権保護システムとして、非特許文献１が公開されている。
【特許文献１】特開２００２－２８１０１３号公報
【非特許文献１】Ｃｏｎｔｅｎｔ　Ｐｒｏｔｅｃｔｉｏｎ　ｆｏｒ　Ｐｒｅｒｅｃｏｒｄｅｄ　Ｍｅｄｉａ　ＤＶＤ　Ｂｏｏｋ、４Ｃ　Ｅｎｔｉｔｙ，ＬＬＣ
【発明の開示】
【発明が解決しようとする課題】

【０００９】
しかしながら、上記したような従来の著作権保護システムでは、対象とするすべての種類の再生装置に対して共通の無効化データを記録媒体に記録するようにしているため、各再生装置はその無効化データ全体を記録媒体から読み込んで少なくとも一時的に格納するメモリを装置内に設ける必要がある。
【００１０】
また、一般に民生用プレーヤにおいては、装置に組み込まれた処理アルゴリズムや鍵の長さを変更することは、時間と手間がかかり困難である。一方、パソコン上のアプリケーションプログラムとして復号処理や鍵がソフトウェアで実装される場合は、一般的にハードウェアで実装する場合に比べて、内蔵する復号アルゴリズムや鍵の更新や追加は容易であるが、復号アルゴリズムや鍵の堅牢な実装は困難である。しかしながら、従来の共通の無効化データを記録媒体に記録する著作権保護システムでは、パソコンのホスト上で動作するアプリケーションプログラムが不正に解析されてアルゴリズムや多数の鍵が暴露された場合であっても、暗号化・復号のアルゴリズムや鍵長を変更することは実質上不可能となっている。これは、無効化機能が正しく働かなくなることを意味し、不正機器によりコンテンツの不正利用が蔓延することにつながる。
【００１１】
本発明では、上記課題を解決するために、再生装置内に設けるメモリのサイズを小さくでき、かつ、パソコンのホスト上で動作するアプリケーションプログラムが不正に解析されてアルゴリズムや多数の鍵が暴露された場合でも、暗号化・復号のアルゴリズムや鍵長を変更することでシステム全体の無効化機能を維持することのできる著作権保護システムを提供する。
【課題を解決するための手段】
【００１２】
本発明は、コンテンツを暗号化して記録する記録装置と、前記暗号化コンテンツを記録する記録媒体と、前記記録媒体に記録された前記暗号化コンテンツを読み出して復号する再生装置とからなる著作権保護システムであって、前記再生装置はＮ個（Ｎは２以上の自然数）のカテゴリに分類されており、前記記録装置は、メディア鍵と前記Ｎ個の各カテゴリに属する再生装置が保有するデバイス鍵データとから前記各カテゴリの特定の再生装置が保有するデバイス鍵を無効化するための無効化データを前記Ｎ個の各カテゴリに対してそれぞれ生成し、前記メディア鍵に基づいて前記コンテンツを暗号化した暗号化コンテンツを生成し、前記Ｎ個の無効化データと前記暗号化コンテンツを前記記録媒体に記録し、前記再生装置は、前記記録媒体から前記Ｎ個の無効化データのうち、前記再生装置が属するカテゴリ用の無効化データ及び前記暗号化コンテンツを読み出し、読み出した前記無効化データに基づいて前記暗号化コンテンツを復号することを特徴とする。
【００１３】
また、本発明は、前記著作権保護システムであって、前記Ｎ個の各無効化データは、対応するカテゴリの再生装置が保有するデバイス鍵データで前記メディア鍵を暗号化した暗号化メディア鍵データであり、前記各カテゴリの再生装置は、前記記録媒体から対応する前記暗号化メディア鍵データ及び前記暗号化コンテンツを読み出し、保有するデバイス鍵で前記暗号化メディア鍵データを復号して前記メディア鍵を取得し、取得した前記メディア鍵に基づいて前記暗号化コンテンツを復号しすることを特徴とする。
【００１４】
また、本発明は、前記著作権保護システムであって、前記記録装置は、前記メディア鍵に基づいて暗号化鍵を生成し、前記暗号化鍵に基づいて前記コンテンツを暗号化し、前記各カテゴリの再生装置は、取得した前記メディア鍵に基づいて復号鍵を生成し、生成した前記復号鍵に基づいて前記暗号化コンテンツを復号することを特徴とする。
【００１５】
また、本発明は、前記著作権保護システムであって、前記記録装置は、コンテンツ鍵で前記コンテンツを暗号化し、前記メディア鍵で前記コンテンツ鍵を暗号化して暗号化コン

テンツ鍵を生成し、生成した前記暗号化コンテンツ鍵を前記記録媒体に記録し、前記各カテゴリの再生装置は、前記記録媒体から前記暗号化コンテンツ鍵を読み出し、前記メディア鍵で前記暗号化コンテンツ鍵を復号してコンテンツ鍵を取得し、取得した前記コンテンツ鍵で前記暗号化コンテンツを復号することを特徴とする。

【００１６】

また、本発明は、前記著作権保護システムであって、前記Ｎ個の各無効化データは対応するカテゴリの再生装置が保有するデバイス鍵データで前記対応するカテゴリ用のメディア鍵を暗号化した暗号化メディア鍵データであり、前記記録装置は、コンテンツ鍵で前記コンテンツを暗号化し、前記コンテンツ鍵を前記Ｎ個のメディア鍵で暗号化してＮ個の暗号化コンテンツ鍵を生成し、前記Ｎ個の暗号化メディア鍵データと前記Ｎ個の暗号化コンテンツ鍵と前記暗号化コンテンツを記録媒体に記録し、前記各カテゴリの再生装置は、前記記録媒体から対応するカテゴリ用の暗号化メディア鍵データと対応するカテゴリ用の暗号化コンテンツ鍵と前記暗号化コンテンツとを読み出し、保有するデバイス鍵で前記暗号化メディア鍵データを復号して前記対応するカテゴリ用のメディア鍵を取得し、取得した前記対応するカテゴリ用のメディア鍵で前記対応するカテゴリ用の暗号化コンテンツ鍵を復号して前記コンテンツ鍵を取得し、取得した前記コンテンツ鍵で前記暗号化コンテンツを復号することを特徴とする。

【００１７】

また、本発明は、コンテンツに暗号化処理を施して記録する記録装置と、前記暗号化コンテンツを記録する記録媒体と、前記記録媒体に記録された前記暗号化コンテンツを読み出して復号する第２のカテゴリの再生装置と、前記記録媒体に記録された前記暗号化コンテンツを読み出して複合処理の一部を行う前記第２のカテゴリの読み出し装置及び前記第２のカテゴリの読み出し装置に接続され前記暗号化コンテンツの複合処理の一部を行う第１のカテゴリの復号装置とから構成される再生装置とからなる著作権保護システムであって、前記記録装置は、メディア鍵と前記第１のカテゴリの復号装置が保有するデバイス鍵データとから前記第１のカテゴリの特定の復号装置が保有するデバイス鍵を無効化するための第１の無効化データを生成し、前記メディア鍵と前記第２のカテゴリの装置が保有するデバイス鍵データとから前記第２のカテゴリの特定の装置が保有するデバイス鍵を無効化するための第２の無効化データを生成し、前記メディア鍵に基づいて前記コンテンツに暗号化処理を施した暗号化コンテンツを生成し、前記第１の無効化データ、前記第２の無効化データ及び前記暗号化コンテンツを前記記録媒体に記録し、前記第２のカテゴリの再生装置は、前記記録媒体から前記第２の無効化データ及び前記暗号化コンテンツを読み出し、前記第２の無効化データに基づいて前記暗号化コンテンツを復号し、前記第２のカテゴリの読み出し装置は、前記記録媒体から前記第１の無効化データ、前記第２の無効化データ及び前記暗号化コンテンツを読み出し、前記第２の無効化データに基づいて前記暗号化コンテンツの復号処理の一部を施した中間データ及び前記第１の無効化データを前記第１カテゴリの復号装置に供給し、前記第１のカテゴリの復号装置は、前記第２のカテゴリの読み出し装置から供給される前記中間データに前記第１の無効化データに基づいて復号処理を施し前記コンテンツを取得することを特徴とする。

【００１８】

また、本発明は、コンテンツを暗号化して記録する記録装置であって、メディア鍵とＮ個（Ｎは２以上の自然数）のカテゴリに分類された各カテゴリに属する再生装置が保有するデバイス鍵データとから前記各カテゴリの特定の再生装置が保有するデバイス鍵を無効化するための無効化データを前記Ｎ個の各カテゴリに対してそれぞれ生成し、前記メディア鍵に基づいて前記コンテンツを暗号化した暗号化コンテンツを生成し、前記Ｎ個の無効化データと前記暗号化コンテンツを前記記録媒体に記録することを特徴とする。

【００１９】

また、本発明は、前記記録装置であって、前記Ｎ個の各無効化データは対応するカテゴリの再生装置が保有するデバイス鍵データで前記メディア鍵を暗号化した暗号化メディア鍵データであることを特徴とする。

【００２０】
また、本発明は、前記記録装置であって、前記メディア鍵に基づいて暗号化鍵を生成し、前記暗号化鍵に基づいて前記コンテンツを暗号化することを特徴とする。
【００２１】
また、本発明は、前記記録装置であって、コンテンツ鍵で前記コンテンツを暗号化し、前記メディア鍵で前記コンテンツ鍵を暗号化した暗号化コンテンツ鍵を生成し、生成した前記暗号化コンテンツ鍵を前記記録媒体に記録することを特徴とする。
【００２２】
また、本発明は、前記記録装置であって、前記Ｎ個の各無効化データは、対応するカテゴリの再生装置が保有するデバイス鍵データで前記対応するカテゴリ用のメディア鍵を暗号化した暗号化メディア鍵データであり、前記記録装置は、コンテンツ鍵で前記コンテンツを暗号化し、前記コンテンツ鍵を前記Ｎ個のメディア鍵で暗号化してＮ個の暗号化コンテンツ鍵データを生成し、前記Ｎ個の暗号化メディア鍵データと前記Ｎ個の暗号化コンテンツ鍵と前記暗号化コンテンツを記録媒体に記録することを特徴とする。
【００２３】
また、本発明は、コンテンツを暗号化して記録する記録装置であって、メディア鍵と第１のカテゴリの復号装置が保有するデバイス鍵データとから前記第１のカテゴリの特定の復号装置が保有するデバイス鍵を無効化するための第１の無効化データを生成し、前記メディア鍵と前記第２のカテゴリの装置が保有するデバイス鍵データとから前記第２のカテゴリの特定の装置が保有するデバイス鍵を無効化するための第２の無効化データを生成し、前記メディア鍵に基づいて前記コンテンツに暗号化処理を施した暗号化コンテンツを生成し、前記第１の無効化データ、前記第２の無効化データ及び前記暗号化コンテンツを前記記録媒体に記録することを特徴とする。
【００２４】
また、本発明は、暗号化コンテンツを記録する記録媒体であって、メディア鍵とＮ個（Ｎは２以上の自然数）のカテゴリに分類された各カテゴリの再生装置が保有するデバイス鍵データとから生成された前記各カテゴリの特定の再生装置が保有するデバイス鍵を無効化するための無効化データと、前記メディア鍵に基づいてコンテンツを暗号化して生成された暗号化コンテンツを記録することを特徴とする。
【００２５】
また、本発明は、前記記録媒体であって、前記Ｎ個の無効化データは、対応するカテゴリの再生装置が保有するデバイス鍵データで前記メディア鍵を暗号化した暗号化メディア鍵データであることを特徴とする。
【００２６】
また、本発明は、前記記録媒体であって、前記暗号化コンテンツは、前記メディア鍵に基づいて生成された暗号化鍵に基づいて前記コンテンツを暗号化して生成されたものであることを特徴とする。
【００２７】
また、本発明は、前記記録媒体であって、前記暗号化コンテンツはコンテンツ鍵で前記コンテンツを暗号化して生成されたものであり、前記メディア鍵で前記コンテンツ鍵を暗号化して生成された暗号化コンテンツ鍵を記録することを特徴とする。
【００２８】
また、本発明は、前記記録媒体であって、前記Ｎ個の各無効化データは、対応するカテゴリの再生装置が保有するデバイス鍵データで前記対応するカテゴリ用のメディア鍵を暗号化した暗号化メディア鍵データであり、前記暗号化コンテンツは、コンテンツ鍵で前記コンテンツを暗号化して生成されたものであり、前記記録媒体は、前記コンテンツ鍵を前記Ｎ個のメディア鍵で暗号化して生成されたＮ個の暗号化コンテンツ鍵を記録することを特徴とする。
【００２９】
また、本発明は、暗号化コンテンツを記録する記録媒体であって、メディア鍵と第１の

カテゴリの復号装置が保有するデバイス鍵データとから生成された前記第１のカテゴリの特定の復号装置が保有するデバイス鍵を無効化するための第１の無効化データと、前記メディア鍵と第２のカテゴリの装置が保有するデバイス鍵データとから生成された前記第２のカテゴリの特定の装置が保有するデバイス鍵を無効化するための第２の無効化データと、前記メディア鍵に基づいて前記コンテンツに暗号化処理を施して生成された暗号化コンテンツとを記録することを特徴とする。

【００３０】

また、本発明は、記録媒体に記録された暗号化コンテンツを再生する再生装置であって、前記再生装置はＮ個（Ｎは２以上の自然数）のカテゴリに分類されており、前記記録媒体には、メディア鍵と前記Ｎ個の各カテゴリの再生装置が保有するデバイス鍵データとから生成された前記各カテゴリの特定の再生装置が保有するデバイス鍵を無効化するための無効化データと、前記メディア鍵に基づいてコンテンツを暗号化して生成された暗号化コンテンツとが記録されており、前記再生装置は、前記記録媒体から前記Ｎ個の無効化データのうち前記再生装置が属するカテゴリ用の無効化データ及び前記暗号化コンテンツを読み出し、読み出した前記無効化データに基づいて前記暗号化コンテンツを復号することを特徴とする。

【００３１】

また、本発明は、前記再生装置であって、前記Ｎ個の各無効化データは、対応するカテゴリの再生装置が保有するデバイス鍵データで前記メディア鍵を暗号化した暗号化メディア鍵データであり、前記再生装置は、前記記録媒体から対応する前記暗号化メディア鍵データ及び前記暗号化コンテンツを読み出し、保有するデバイス鍵で前記暗号化メディア鍵データを復号して前記メディア鍵を取得し、取得した前記メディア鍵に基づいて前記暗号化コンテンツを復号することを特徴とする。

【００３２】

また、本発明は、前記再生装置であって、前記暗号化コンテンツは、前記メディア鍵に基づいて生成された暗号化鍵に基づいて前記コンテンツを暗号化して生成されたものであり、前記再生装置は、取得した前記メディア鍵に基づいて復号鍵を生成し、生成した前記復号鍵に基づいて前記暗号化コンテンツを復号することを特徴とする。

【００３３】

また、本発明は、前記再生装置であって、前記暗号化コンテンツは、コンテンツ鍵で前記コンテンツを暗号化して生成されたものであり、前記記録媒体には、前記メディア鍵で前記コンテンツ鍵を暗号化して生成された暗号化コンテンツ鍵が記録されており、前記再生装置は、前記記録媒体から前記暗号化コンテンツ鍵を読み出し、前記メディア鍵で前記暗号化コンテンツ鍵を復号してコンテンツ鍵を取得し、取得した前記コンテンツ鍵で前記暗号化コンテンツを復号することを特徴とする。

【００３４】

また、本発明は、前記再生装置であって、前記Ｎ個の無効化データは、対応するカテゴリの再生装置が保有するデバイス鍵データで前記対応するカテゴリ用のメディア鍵を暗号化した暗号化メディア鍵データであり、前記暗号化コンテンツは、コンテンツ鍵で前記コンテンツを暗号化して生成されたものであり、前記記録媒体には、前記コンテンツ鍵を前記Ｎ個のメディア鍵で暗号化して生成されたＮ個の暗号化コンテンツ鍵が記録されており、前記再生装置は、前記記録媒体から対応するカテゴリ用の暗号化メディア鍵データと対応するカテゴリ用の暗号化コンテンツ鍵と前記暗号化コンテンツとを読み出し、保有するデバイス鍵で前記暗号化メディア鍵データを復号して前記対応するカテゴリ用のメディア鍵を取得し、取得した前記対応するカテゴリ用のメディア鍵で前記暗号化コンテンツ鍵を復号して前記コンテンツ鍵を取得し、取得した前記コンテンツ鍵で前記暗号化コンテンツを復号することを特徴とする。

【００３５】

また、本発明は、記録媒体に記録された暗号化コンテンツを再生する再生装置であって、前記記録媒体には、メディア鍵と第１のカテゴリの復号装置が保有するデバイス鍵デー

タとから生成された前記第１のカテゴリの特定の復号装置が保有するデバイス鍵を無効化するための第１の無効化データと、前記メディア鍵と第２のカテゴリの装置が保有するデバイス鍵データとから生成された前記第２のカテゴリの特定の装置が保有するデバイス鍵を無効化するための第２の無効化データと、前記メディア鍵に基づいて暗号化処理を施して生成された暗号化コンテンツとが記録されており、前記再生装置は、前記第２のカテゴリに属し、前記記録媒体から前記第２の無効化データ及び前記暗号化コンテンツを読み出し、前記第２の無効化データに基づいて前記暗号化コンテンツを復号することを特徴とする。

【００３６】

また、本発明は、記録媒体に記録された暗号化コンテンツを再生する再生装置を構成する読み出し装置であって、前記記録媒体には、メディア鍵と第１のカテゴリの復号装置が保有するデバイス鍵データとから生成された前記第１のカテゴリの特定の復号装置が保有するデバイス鍵を無効化するための第１の無効化データと、前記メディア鍵と第２のカテゴリの装置が保有するデバイス鍵データとから生成された前記第２のカテゴリの特定の装置が保有するデバイス鍵を無効化するための第２の無効化データと、前記メディア鍵に基づいて暗号化処理を施して生成された暗号化コンテンツとが記録されており、前記読み出し装置は、前記第２のカテゴリに属し、前記記録媒体から前記第１の無効化データ、前記第２の無効化データ及び前記暗号化コンテンツを読み出し、前記第２の無効化データに基づいて前記暗号化コンテンツの復号処理の一部を施した中間データを生成し、生成した前記中間データ及び前記第１の無効化データを出力することを特徴とする。

【００３７】

また、本発明は、記録媒体に記録された暗号化コンテンツを再生する再生装置を構成する復号装置であって、前記記録媒体には、メディア鍵と第１のカテゴリの復号装置が保有するデバイス鍵データとから生成された前記第１のカテゴリの特定の復号装置が保有するデバイス鍵を無効化するための第１の無効化データと、前記メディア鍵と第２のカテゴリの装置が保有するデバイス鍵データとから生成された前記第２のカテゴリの特定の装置が保有するデバイス鍵を無効化するための第２の無効化データと、前記メディア鍵に基づいて暗号化処理を施して生成された暗号化コンテンツとが記録されており、前記第２のカテゴリの読み出し装置は、前記記録媒体から前記第１の無効化データ、前記第２の無効化データ及び前記暗号化コンテンツを読み出し、前記第２の無効化データに基づいて前記暗号化コンテンツの復号処理の一部を施した中間データを生成し、生成した前記中間データ及び前記第１の無効化データを出力し、前記復号装置は、前記第１のカテゴリに属し、前記第２のカテゴリの読み出し装置から供給される前記中間データに前記第１の無効化データに基づいて復号処理を施して前記コンテンツを取得することを特徴とする。

【００３８】

また、本発明は、記録媒体に記録された暗号化コンテンツを再生する再生装置であって、
請求項２５記載の読み取り装置と請求項２６記載の復号装置とから構成されることを特徴とする。

【００３９】

また、本発明は、コンテンツを暗号化及び復号するために必要な無効化データを生成して記録する鍵生成装置と、コンテンツを暗号化して記録する記録装置と、前記無効化データと前記暗号化コンテンツを記録する記録媒体と、前記記録媒体に記録された前記暗号化コンテンツを読み出して復号する再生装置とからなる著作権保護システムであって、前記記録装置及び前記再生装置はＮ個（Ｎは２以上の自然数）のカテゴリに分類されており、前記鍵生成装置は、メディア鍵と前記各カテゴリに属する記録装置もしくは再生装置が保有するデバイス鍵データとから前記各カテゴリの特定の記録装置もしくは再生装置が保有するデバイス鍵を無効化するための無効化データを、前記Ｎ個の各カテゴリに対してそれぞれ生成し、生成した前記Ｎ個の無効化データを前記記録媒体に記録し、前記記録装置は、前記記録媒体から前記Ｎ個の無効化データのうち、前記記録装置が属するカテゴリ用の

無効化データを読み出し、読み出した前記無効化データに基づいてコンテンツを暗号化して暗号化コンテンツを生成し、生成した前記暗号化コンテンツを前記記録媒体に記録し、前記再生装置は、前記記録媒体から前記Ｎ個の無効化データのうち、前記再生装置が属するカテゴリ用の無効化データ及び前記暗号化コンテンツを読み出し、読み出した前記無効化データに基づいて前記暗号化コンテンツを復号することを特徴とする。

【００４０】

また、本発明は、鍵生成装置であって、メディア鍵とＮ個（Ｎは２以上の自然数）のカテゴリに分類された各カテゴリに属する記録装置もしくは再生装置が保有するデバイス鍵データとから前記各カテゴリの特定の記録装置もしくは再生装置が保有するデバイス鍵を無効化するための無効化データを、前記Ｎ個の各カテゴリに対してそれぞれ生成し、生成した前記Ｎ個の無効化データを前記記録媒体に記録することを特徴とする。

【００４１】

また、本発明は、コンテンツを暗号化して記録する記録装置であって、メディア鍵とＮ個（Ｎは２以上の自然数）のカテゴリに分類された各カテゴリに属する記録装置もしくは再生装置が保有するデバイス鍵データとから生成された前記各カテゴリの特定の記録装置もしくは再生装置が保有するデバイス鍵を無効化するための無効化データが記録された記録媒体から、前記Ｎ個の無効化データのうち前記記録装置が属するカテゴリ用の無効化データを読み出し、読み出した前記無効化データに基づいてコンテンツを暗号化して暗号化コンテンツを生成し、生成した前記暗号化コンテンツを前記記録媒体に記録することを特徴とする。

【発明の効果】

【００４２】

本発明によれば、第１のカテゴリの装置及び第２のカテゴリの装置は、それぞれ異なるカテゴリの装置を無効化するための第１もしくは第２の暗号化メディア鍵を読み込む必要がないため、装置内に設けるメモリ容量を小さくでき、処理時間も短くできる。また、第１の暗号化メディア鍵の生成に用いる暗号化アルゴリズムを第２の暗号化メディア鍵の生成に用いる暗号化アルゴリズムと異なるものとすることができるため、第１のカテゴリの再生装置の無効化システムが暴露されるような事態に陥った場合にも、第１のカテゴリの再生装置に付与するデバイス鍵の鍵長や第１の暗号化メディア鍵の生成アルゴリズムを変更することで、第２のカテゴリの再生装置に影響を与えることなく、無効化システムを更新することができる。

【発明を実施するための最良の形態】

【００４３】

以下、本発明の実施の形態について、図面を参照にしながら説明する。

【００４４】

（実施の形態１）

本発明の実施の形態１は、再生専用の記録媒体を用いてコンテンツを配布し、再生装置でコンテンツを再生するシステムに本発明を適用したものである。

【００４５】

以下、本発明の実施の形態１について、図面を参照しながら説明する。図１は、コンテンツを暗号化して記録する記録装置１００及び記録媒体１２０を示しており、図２は、記録媒体１２０から暗号化コンテンツを読み出して復号する第１のカテゴリの再生装置２００を示しており、図３は、記録媒体１２０から暗号化コンテンツを読み出して復号する第２のカテゴリの再生装置３００を示している。また、図４は記録媒体１２０に記録される各種データの具体例を示している。

【００４６】

記録装置１００は、第１のカテゴリの各再生装置が秘密に保有するデバイス鍵を格納する第１のデバイス鍵格納部１０１と、第２のカテゴリの各再生装置が秘密に保有するデバイス鍵を格納する第２のデバイス鍵格納部１０２と、メディア鍵を暗号化するために用いるデバイス鍵を選択する第１のデバイス鍵選択部１０３及び第２のデバイス鍵選択部１０

４と、外部から入力されるメディア鍵を第１のデバイス鍵選択部１０３で選択したデバイス鍵で暗号化する第１のメディア鍵暗号化部１０５と、メディア鍵を第２のデバイス鍵選択部１０４で選択したデバイス鍵で暗号化する第２のメディア鍵暗号化部１０６と、外部から入力されるコンテンツ鍵をメディア鍵で暗号化するコンテンツ鍵暗号化部１０７と、同じく外部から入力されるコンテンツを暗号化するコンテンツ暗号化部１０８とを備える。

【００４７】

なお、図１には示していないが、第１のメディア鍵暗号化部１０５には、第１のカテゴリの再生装置のうち無効化すべき再生装置の情報が、第２のメディア鍵暗号化部１０６には第２のカテゴリの再生装置のうち無効化すべき再生装置の情報が、それぞれ入力されており、暗号化メディア鍵を生成する際にこれら無効化すべき再生装置では正しいメディア鍵が復号できないように暗号化メディア鍵を生成する。さらにメディア鍵は記録媒体を製造する度に、コンテンツ鍵はコンテンツ毎に異なる鍵データを選択している。

【００４８】

記録媒体１２０は、第１のメディア鍵暗号化部１０５が生成した第１の暗号化メディア鍵データを記録する第１の暗号化メディア鍵データ記録領域１２１と、第２のメディア鍵暗号化部１０６が生成した第２の暗号化メディア鍵データを記録する第２の暗号化メディア鍵データ記録領域１２２と、コンテンツ鍵暗号化部１０７が生成した暗号化コンテンツ鍵を記録する暗号化コンテンツ鍵記録領域１２３と、コンテンツ暗号化部１０８が生成した暗号化コンテンツを記録する暗号化コンテンツ記録領域１２４とを備える。

【００４９】

第１のカテゴリの再生装置２００は、デバイス鍵を秘密に保有するデバイス鍵格納部２０１と、デバイス鍵を用いて記録媒体１２０から読み出した第１の暗号化メディア鍵データを復号してメディア鍵を取得するメディア鍵復号部２０２と、取得したメディア鍵を用いて記録媒体１２０から読み出した暗号化コンテンツ鍵を復号してコンテンツ鍵を取得するコンテンツ鍵復号部２０３と、取得したコンテンツ鍵を用いて記録媒体１２０から読み出した暗号化コンテンツを復号するコンテンツ復号部２０４とを備える。本実施の形態ではパソコン上のアプリケーションプログラムのようにソフトウェアで実装される再生装置を第１のカテゴリに属する再生装置とした。

【００５０】

第２のカテゴリの再生装置３００は、デバイス鍵を秘密に保有するデバイス鍵格納部３０１と、デバイス鍵を用いて記録媒体１２０から読み出した第２の暗号化メディア鍵データを復号してメディア鍵を取得するメディア鍵復号部３０２と、取得したメディア鍵を用いて記録媒体１２０から読み出した暗号化コンテンツ鍵を復号してコンテンツ鍵を取得するコンテンツ鍵復号部３０３と、取得したコンテンツ鍵を用いて記録媒体１２０から読み出した暗号化コンテンツを復号するコンテンツ復号部３０４とを備える。本実施の形態では一般的な民生プレーヤのようにハードウェアで実装される再生装置を第２のカテゴリに属する再生装置とした。

【００５１】

図４は、ｍ台の第１のカテゴリの再生装置及びｎ台の第２のカテゴリの再生装置がそれぞれ固有のデバイス鍵を１個だけ保有しており、第１のカテゴリの再生装置２と第２のカテゴリの再生装置３が無効化されているとした場合の、記録媒体１２０に記録される各種データの具体例を示している。図４中で、第１のカテゴリの再生装置ｉ（ｉ＝１～ｍ）が保有するデバイス鍵をＤＫＡｉ、第２のカテゴリの再生装置ｊ（ｊ＝１～ｎ）が保有するデバイス鍵をＤＫＢｊとしている。また、Ｅａ（Ｘ，Ｙ）、Ｅｂ（Ｘ，Ｙ）、Ｅｃ（Ｘ，Ｙ）及びＥｄ（Ｘ，Ｙ）はデータＹを鍵データＸを用いて暗号化する関数を意味する。なお、使用される暗号アルゴリズムは、公知の技術で実現可能であり、本実施の形態では鍵長５６ｂｉｔのＤＥＳ暗号を使用した。

【００５２】

（第１の暗号化メディア鍵データ記録領域１２１）

第１の暗号化メディア鍵データ記録領域１２１には、第１のカテゴリの再生装置が保有するデバイス鍵（ＤＫＡ１～ＤＫＡｍ）で暗号化されたメディア鍵（ＭＫ）が記録されている。ここで、第１のカテゴリの再生装置２は無効化されており、ＤＫＡ２ではメディア鍵（ＭＫ）とはまったく無関係のデータ「０」が暗号化されて記録されている。これは第１の暗号化メディア鍵を生成する際に、第１のメディア鍵暗号化部１０５において、第１のカテゴリのうち無効化すべき再生装置の情報として再生装置２が入力され、再生装置２では正しいメディア鍵が得られないように処理された結果である。

【００５３】

（第２の暗号化メディア鍵データ記録領域１２２）

第２の暗号化メディア鍵データ記録領域１２２には、第２のカテゴリの再生装置が保有するデバイス鍵（ＤＫＢ１～ＤＫＢｎ）で暗号化されたメディア鍵（ＭＫ）が記録されている。ここで、第２のカテゴリの再生装置３は無効化されており、ＤＫＢ３ではメディア鍵（ＭＫ）とはまったく無関係のデータ「０」が暗号化されて記録されている。これは第２の暗号化メディア鍵を生成する際に、第２のメディア鍵暗号化部１０６において、第２のカテゴリのうち無効化すべき再生装置の情報として再生装置３が入力され、再生装置３では正しいメディア鍵が得られないように処理された結果である。

【００５４】

第１及び第２の暗号化メディア鍵データをこのように生成することにより、第１のカテゴリの再生装置２及び第２のカテゴリの再生装置３を除く再生装置が正しいメディア鍵（ＭＫ）を復号することができるとともに、第１のカテゴリの再生装置２及び第２のカテゴリの再生装置３をシステムから排除することができる。

【００５５】

（暗号化コンテンツ鍵記録領域１２３）

暗号化コンテンツ鍵記録領域１２３にはメディア鍵（ＭＫ）で暗号化されたコンテンツ鍵（ＣＫ）が記録されている。

【００５６】

（暗号化コンテンツ記録領域１２４）

暗号化コンテンツ記録領域１２４には、コンテンツ鍵（ＣＫ）で暗号化されたコンテンツが記録されている。

【００５７】

以上のように構成された本発明の実施の形態１において、例えば第１のカテゴリの再生装置に付与したデバイス鍵の多数や、第１の暗号化メディア鍵データを復号するアルゴリズムがインターネット上で不正に公開され、第１のカテゴリの再生装置の無効化が機能しなくなったと判断された場合には、第１のカテゴリの再生装置の無効化システムを更新することになる。以下、その具体例を説明する。

【００５８】

（システム更新の具体例１）

第１のカテゴリの再生装置の無効化が機能しなくなったと判断されて以降、新たに作成する記録媒体１２０に記録する各種データの具体例１を図５に示す。図４との違いは、第１の暗号化メディア鍵データの生成に用いるデバイス鍵をＤＫＡ１～ＤＫＡｍからＤＫＡ’１～ＤＫＡ’ｍに変更したことである。ここで、新たなデバイス鍵（ＤＫＡ’１～ＤＫＡ’ｍ）のうちの各デバイス鍵は、システム更新前のデバイス鍵（ＤＫＡ１～ＤＫＡｍ）のどれとも一致しないようになっている。

【００５９】

一方、無効化されていない第１のカテゴリの再生装置２００には、新たなデバイス鍵が付与され、デバイス鍵格納部２０１に格納される。例えば、第１のカテゴリの再生装置ｍは、以前から保有していたデバイス鍵（ＤＫＡｍ）に加え、新たに付与されたデバイス鍵（ＤＫＡ’ｍ）をデバイス鍵格納部２０１に保有する。再生装置ｍは、図４の記録媒体を再生する際には、デバイス鍵ＤＫＡｍを用い、無効化システム更新後の図５の記録媒体を再生する際には、デバイス鍵ＤＫＡ’ｍを用いて、記録媒体から読み出した第１の暗号化

メディア鍵を復号してメディア鍵（ＭＫ）を取得し、取得したメディア鍵（ＭＫ）を用いて暗号化コンテンツ鍵を復号してコンテンツ鍵（ＣＫ）を取得し、取得したコンテンツ鍵（ＣＫ）を用いて暗号化コンテンツを復号再生する。

【００６０】

ここで、新たなデバイス鍵（ＤＫＡ’１～ＤＫＡ’ｍ）のうちの各デバイス鍵は、システム更新前のデバイス鍵（ＤＫＡ１～ＤＫＡｍ）のどれとも一致しないようになっているので、システム更新前に不正な解析行為により暴露されたデバイス鍵がＤＫＡ２以外に存在したとしても、そのデバイス鍵を使って図５の記録媒体から読み出した第１の暗号化メディア鍵を復号してメディア鍵（ＭＫ）を取得することはできず、コンテンツを再生することはできない。

【００６１】

なお、上記したシステム更新に際して、第２の暗号化メディア鍵データの生成に用いるデバイス鍵（ＤＫＢ１～ＤＫＢｎ）は変更されていないので、第２のカテゴリに属する再生装置には何らの変更を加える必要がない。

【００６２】

（システム更新の具体例２）

第１のカテゴリの再生装置の無効化が機能しなくなったと判断されて以降、新たに作成する記録媒体１２０に記録する各種データの具体例２を図６に示す。図４との違いは、第１の暗号化メディア鍵の生成に用いるデバイス鍵をＤＫＡ１～ＤＫＡｍからＤＫＡ’１～ＤＫＡ’ｍに変更したことと、暗号化アルゴリズムをＥａ（Ｘ，Ｙ）からＥａ’（Ｘ，Ｙ）に変更したことである。ここで、新たなデバイス鍵（ＤＫＡ’１～ＤＫＡ’ｍ）のうちの各デバイス鍵は、システム更新前のデバイス鍵（ＤＫＡ１～ＤＫＡｍ）のどれとも一致しないようになっている。

【００６３】

一方、無効化されていない第１のカテゴリの各再生装置２００には、新たなデバイス鍵を付与されデバイス鍵格納部２０１に格納される。また、メディア鍵復号部２０２には、以前から組み込まれている図４の第１の暗号化メディア鍵データを復号するための復号アルゴリズムＤａ（Ｘ，Ｙ）に加えて、図５の第１の暗号化メディア鍵データを復号するための復号アルゴリズムＤａ’（Ｘ，Ｙ）が組み込まれる。例えば、第１のカテゴリの再生装置ｍは、以前から保有していたデバイス鍵（ＤＫＡｍ）に加え、新たに付与されたデバイス鍵（ＤＫＡ’ｍ）を保有する。再生装置ｍは、図４の記録媒体を再生する際には、デバイス鍵ＤＫＡｍと暗号化アルゴリズムＤａ（Ｘ，Ｙ）を用い、図５の記録媒体を再生する際には、デバイス鍵ＤＫＡ’ｍと暗号アルゴリズムＤａ’（Ｘ，Ｙ）を用いて、記録媒体から読み出した第１の暗号化メディア鍵データを復号してメディア鍵（ＭＫ）を取得し、取得したメディア鍵（ＭＫ）を用いて暗号化コンテンツ鍵を復号してコンテンツ鍵（ＣＫ）を取得し、取得したコンテンツ鍵（ＣＫ）を用いて暗号化コンテンツを復号する。本実施の形態ではＥａ（Ｘ，Ｙ）及びＤａ（Ｘ，Ｙ）は鍵長５６ｂｉｔのＤＥＳ暗号を用いたのに対して、Ｅａ’（Ｘ，Ｙ）及びＤａ’（Ｘ，Ｙ）では２キートリプルＤＥＳと呼ばれる鍵長１１２ｂｉｔの暗号を用いた。

【００６４】

ここで、新たなデバイス鍵（ＤＫＡ’１～ＤＫＡ’ｍ）のうちの各デバイス鍵は、システム更新前のデバイス鍵（ＤＫＡ１～ＤＫＡｍ）のどれとも一致しないようになっているので、システム更新前に不正な解析行為により暴露されたデバイス鍵がＤＫＡ２以外に存在したとしても、そのデバイス鍵を使って図５の記録媒体から読み出した第１の暗号化メディア鍵データを復号してメディア鍵（ＭＫ）を取得することはできず、コンテンツを再生することはできない。

【００６５】

また、デバイス鍵の鍵長や暗号アルゴリズムを変更して暗号強度の高いものにすることができるので、システムを解析してデバイス鍵を不正取得するといった行為を困難にすることができる。

【００６６】
なお、上記したシステム更新に際して、第２の暗号化メディア鍵データの生成に用いるデバイス鍵（ＤＫＢ１～ＤＫＢｎ）及び第２の暗号化メディア鍵データの暗号化アルゴリズムは変更されていないので、第２のカテゴリに属する再生装置には何らの変更を加える必要がない。
【００６７】
なお、システム更新の具体例１、２ともに記録媒体にはシステム更新の世代に関する情報を記録しており、第１のカテゴリの再生装置はこの情報に基づいて、いずれの世代のデバイス鍵あるいはアルゴリズムを使用するかを判断する。
【００６８】
以上のように構成された本発明の実施の形態１によれば、第１のカテゴリの再生装置２００及び第２のカテゴリの再生装置３００は、それぞれ異なるカテゴリの再生装置を無効化するための第１もしくは第２の暗号化メディア鍵データを読み込む必要がないため、装置内に設けるメモリ容量を小さくでき、処理時間も短くできる。また、第１の暗号化メディア鍵データの生成に用いる暗号化アルゴリズムを第２の暗号化メディア鍵データの生成に用いる暗号化アルゴリズムと異なるものとすることができるため、第１のカテゴリの再生装置の無効化システムが暴露されるような事態に陥った場合にも、第１のカテゴリの再生装置に付与するデバイス鍵の鍵長や第１の暗号化メディア鍵データの生成アルゴリズムを変更することで、第２のカテゴリの再生装置に影響を与えることなく、無効化システムを変更することが可能になる。これは、本実施の形態のように第１のカテゴリは復号アルゴリズムや鍵の更新や追加が容易ではあるが堅牢な実装が困難なソフトウェアで実装される再生装置とし、第２のカテゴリは堅牢ではあるが復号アルゴリズムや鍵の更新や追加が困難なハードウェアで実装される再生装置とした場合に、特に有効である。
【００６９】
なお、本実施の形態では図１において、メディア鍵及びコンテンツ鍵が記録装置１００の外部から入力される形態としたが、本発明はその構成に限定されるものではない。例えば、記録装置１００がメディア鍵及びコンテンツ鍵を格納する格納部を有する構成であってもよい。また、記録装置１００がメディア鍵及びコンテンツ鍵をその都度生成する生成部を有する構成であってもよい。
【００７０】
また、本実施の形態では図１において、コンテンツをコンテンツ鍵で暗号化し、コンテンツ鍵をメディア鍵で暗号化する２階層の構成としたが、本発明はそれに限定されるものではない。例えば、メディア鍵で直接コンテンツを暗号化する１階層の構成であってもよい。また、鍵を追加して暗号化の階層をさらに増やす構成であってもよい。
【００７１】
また、本実施の形態では記録装置として図１に示すように、各カテゴリのデバイス鍵格納部、メディア鍵暗号化部、コンテンツ鍵暗号化部、コンテンツ暗号化部及び記録媒体への各データの記録が一体の構成としたが、本発明はそれに限定されるものではなく、記録装置が分離して構成されるものであっても良い。例えば、各カテゴリのデバイス鍵格納部、メディア鍵暗号化部、及びコンテンツ鍵暗号化部（図１中の破線で囲んだ部分）は、その管理、運用に高い秘匿性が要求されることから、システム全体の鍵管理や再生装置に対する鍵発行等を運用する機関に設置される装置に内蔵され、コンテンツ暗号化部や記録媒体への各データの記録はコンテンツ製造機関や記録媒体製造機関に設置される装置で実行される形態であっても良い。
【００７２】
また、本実施の形態ではシステム更新において第１の暗号化メディア鍵データを生成する際に、図５のＥａ（ＤＫＡ’２，０）や図６のＥａ’（ＤＫＡ’２，０）のようにシステム更新の時点で無効化されている再生装置にもデータを割り当てる構成としているが、無効化されている再生装置にはデータを割り当てない構成とすることも可能である。その場合、無効化されていない再生装置の使うべき暗号化メディア鍵の位置も更新し、新たな

デバイス鍵を付与する際に新たな位置情報も付与することで、システム更新の前後において暗号化メディア鍵の位置が変わったとしても無効化されていない再生装置は適切なデータを用いることができ、正しいメディア鍵を得ることができる。こうした場合、システム更新後の第１の暗号化メディア鍵データ記録領域に格納すべきデータの容量を削減することができる。あるいは容量の最大値が限定されている場合は新たに第１のカテゴリに属する再生装置の台数を増やすことが可能となる。

【００７３】

また、本実施の形態では、図４に示すような暗号化メディア鍵データを用いて再生装置の無効化を行う方法としたが、無効化の方法は他の方法を利用してもよく、例えば特許文献１として開示されている木構造を利用した無効化方法を用いても良い。

【００７４】

また、本実施の形態では、暗号アルゴリズムとして鍵長５６ｂｉｔのＤＥＳ、あるいはシステム更新後の暗号アルゴリズムとして鍵長１１２ｂｉｔの２キートリプルＤＥＳを用いたが、本発明はこれに限定されるものではなく、他の暗号アルゴリズム、例えば次世代の標準暗号とされる鍵長１２８ｂｉｔのＡＥＳ等を用いても良い。

【００７５】

（実施の形態２）

本発明の実施の形態２は、書き換え型もしくは追記型の記録媒体に記録装置でコンテンツを記録し、再生装置でコンテンツを再生するシステムに本発明を適用したものである。

【００７６】

以下、本発明の実施の形態２について、図面を参照しながら説明する。図７は、鍵情報を生成して記録する鍵生成装置７００及び記録媒体７２０を示しており、図８は、記録媒体７２０にコンテンツを暗号化して記録する第１のカテゴリの記録装置８００を示しており、図９は、記録媒体７２０にコンテンツを暗号化して記録する第２のカテゴリの記録装置９００を示しており、図１０は記録媒体７２０から暗号化コンテンツを読み出して復号する第１のカテゴリの再生装置１０００を示しており、図１１は記録媒体７２０から暗号化コンテンツを読み出して復号する第２のカテゴリの再生装置１１００を示している。また、図１２は、記録媒体７２０に記録される各種データの具体例を示している。

【００７７】

鍵生成装置７００は、第１のデバイス鍵格納部７０１に第１のカテゴリの各装置が秘密に保有するデバイス鍵を、第２のデバイス鍵格納部７０２に第２のカテゴリの各装置が秘密に保有するデバイス鍵を、それぞれ格納する。メディア鍵及びコンテンツ鍵の暗号化については、前記した実施の形態１における記録装置と同様であるので、その説明は省略する。

【００７８】

記録媒体７２０は、第１の暗号化メディア鍵データ記録領域７２１と、第２の暗号化メディア鍵データ記録領域７２２と、暗号化コンテンツ鍵記録領域７２３と、暗号化コンテンツ記録領７２４とを備える。ここで、破線で囲んだ、第１の暗号化メディア鍵データ記録領域７２１、第２の暗号化メディア鍵データ記録領域７２２、及び、暗号化コンテンツ鍵記録領域７２３は、第１のカテゴリの記録装置８００及び第２のカテゴリの記録装置９００では記録不可能な領域である。一方、暗号化コンテンツ記録領域は、第１のカテゴリの記録装置８００及び第２のカテゴリの記録装置９００で記録可能な領域である。

【００７９】

第１のカテゴリの記録装置８００は、デバイス鍵を秘密に保有するデバイス鍵格納部８０１と、デバイス鍵を用いて記録媒体７２０から読み出した第１の暗号化メディア鍵データを復号してメディア鍵を取得するメディア鍵復号部８０２と、取得したメディア鍵を用いて記録媒体から読み出した暗号化コンテンツ鍵を復号してコンテンツ鍵を取得するコンテンツ鍵復号部８０３と、取得したコンテンツ鍵を用いて外部から入力されたコンテンツを暗号化するコンテンツ暗号化部８０４とを備える。本実施の形態では、パソコン上のアプリケーションプログラムのようにソフトウェアで実装される記録装置を第１のカテゴリ

に属する記録装置とした。

【００８０】

第２のカテゴリの記録装置９００は、デバイス鍵を秘密に保有するデバイス鍵格納部９０１と、デバイス鍵を用いて記録媒体７２０から読み出した第２の暗号化メディア鍵データを復号してメディア鍵を取得するメディア鍵復号部９０２と、取得したメディア鍵を用いて記録媒体から読み出した暗号化コンテンツ鍵を復号してコンテンツ鍵を取得するコンテンツ鍵復号部９０３と、取得したコンテンツ鍵を用いて外部から入力されたコンテンツを暗号化するコンテンツ暗号化部９０４とを備える。本実施の形態では、一般的な民生レコーダのようにハードウェアで実装される記録装置を第２のカテゴリに属する記録装置とした。

【００８１】

第１のカテゴリの再生装置１０００及び第２のカテゴリの再生装置１１００は、それぞれ前記した本発明の実施の形態１における第１のカテゴリの再生装置２００及び第２のカテゴリの再生装置３００と同じ構成であり、同一の構成要素には同一の符号を付し、その説明を省略する。

【００８２】

図１２は、ｍ台の第１のカテゴリの装置、及びｎ台の第２のカテゴリの装置がそれぞれ固有のデバイス鍵を１個だけ保有しており、第１のカテゴリの装置２と第２のカテゴリの装置３が無効化されているとした場合の、記録媒体７２０に記録される各種データの具体例を示している。図１２中で、第１のカテゴリの装置ｉ（ｉ＝１～ｍ）が保有するデバイス鍵をＤＫＡｉ、第２のカテゴリの装置ｊ（ｊ＝１～ｎ）が保有するデバイス鍵をＤＫＢｊとしている。なお、第１の暗号化メディア鍵データ記録領域７２１、第２の暗号化メディア鍵データ記録領域７２２、暗号化コンテンツ鍵データ記録領域７２３、及び暗号化コンテンツ記録領域７２４に記録されるデータは、それぞれ前記した本発明の実施の形態１における第１の暗号化メディア鍵データ記録領域１２１、第２の暗号化メディア鍵データ記録領域１２２、暗号化コンテンツ鍵データ記録領域１２３、及び暗号化コンテンツ記録領域１２４に記録されるデータと同じであるので、その説明を省略する。

【００８３】

本実施の形態によれば、上記した構成により、第１のカテゴリの装置２及び第２のカテゴリの装置３を除く装置が正しいメディア鍵（ＭＫ）を復号することができるとともに、第１のカテゴリの装置２及び第２のカテゴリの装置３をシステムから排除することができる。

【００８４】

また、本実施の形態において、第１のカテゴリの装置の無効化が機能しなくなったと判断された場合には、第１のカテゴリの装置の無効化システムを更新することになる。更新の方法については、前記した本発明の実施の形態１の場合と同様の方法がとれるので、その説明を省略する。

【００８５】

なお、システムの更新に際して、第２の暗号化メディア鍵の生成に用いるデバイス鍵（ＤＫＢ１～ＤＫＢｎ）は変更されていないので、第２のカテゴリに属する記録装置及び再生装置には何らの変更を加える必要がない。

【００８６】

以上のように構成された本発明の実施の形態２によれば、第１のカテゴリの装置（記録装置８００及び再生装置１０００）及び第２のカテゴリの装置（記録装置９００及び再生装置１１００）は、それぞれ異なるカテゴリの装置を無効化するための第１もしくは第２の暗号化メディア鍵データを読み込む必要がないため、装置内に設けるメモリ容量を小さくでき、処理時間も短くできる。また、第１の暗号化メディア鍵データの生成に用いる暗号化アルゴリズムを第２の暗号化メディア鍵データの生成に用いる暗号化アルゴリズムと異なるものとすることができるため、第１のカテゴリの装置の無効化システムが暴露されるような事態に陥った場合にも、第１のカテゴリの装置に付与するデバイス鍵の鍵長や第

１の暗号化メディア鍵データの生成アルゴリズムを変更することで、第２のカテゴリの装置に影響を与えることなく、無効化システムを変更することが可能になる。これは、本実施の形態のように第１のカテゴリは復号アルゴリズムや鍵の更新や追加が容易ではあるが堅牢な実装が困難なソフトウェアで実装される装置とし、第２のカテゴリは堅牢ではあるが復号アルゴリズムや鍵の更新や追加が困難なハードウェアで実装される装置とした場合に、特に有効である。

【００８７】

なお、本実施の形態では、各カテゴリの記録装置と再生装置が別々の装置である形態としたが、本発明はそれに限定されるものではない。例えば、記録装置と再生装置が同一の装置である形態であっても良い。

【００８８】

また、本実施の形態では図７において、メディア鍵及びコンテンツ鍵が鍵生成装置７００の外部から入力される形態としたが、本発明はその構成に限定されるものではない。例えば、鍵生成装置７００がメディア鍵及びコンテンツ鍵を格納する格納部を有する構成であってもよい。また、鍵生成装置７００がメディア鍵及びコンテンツ鍵をその都度生成する生成部を有する構成であってもよい。

【００８９】

また、本実施の形態では図８及び図９において、メディア鍵で暗号化コンテンツ鍵を復号してコンテンツ鍵を取得し、取得したコンテンツ鍵でコンテンツを暗号化する２階層の構成としたが、本発明はそれに限定されるものではない。例えば、メディア鍵で直接コンテンツを暗号化する１階層の構成であってもよい。また、記録装置内部で生成したコンテンツ鍵を用いてコンテンツを暗号化し、コンテンツ鍵をメディア鍵で暗号化し、暗号化コンテンツと暗号化コンテンツ鍵を記録媒体に記録する構成であってもよい。また、鍵を追加して暗号化の階層をさらに増やす構成であってもよい。

【００９０】

また、本実施の形態では鍵生成装置として図７に示すように、各カテゴリのデバイス鍵格納部、メディア鍵暗号化部、コンテンツ鍵暗号化部、及び記録媒体への各データの記録が一体の構成としたが、本発明はそれに限定されるものではない。例えば、各カテゴリのデバイス鍵格納部、メディア鍵暗号化部、及びコンテンツ鍵暗号化部は、その管理、運用に高い秘匿性が要求されることから、システム全体の鍵管理や再生装置に対する鍵発行等を運用する機関に設置される装置に内蔵され、記録媒体への各データの記録は記録媒体製造機関に設置される装置で実行される形態であっても良い。一般的に書き換え型もしくは追記型の光ディスクでは、一般ユーザの保有する記録装置で記録可能な領域と、一般ユーザの保有する記録装置では記録不可能な再生専用領域を備えており、この再生専用領域にはディスク製造業者が出荷前にデータを記録する。この場合、ディスク製造業者による再生専用領域へのデータ記録は、スタンパと呼ばれる原盤にデータを記録し、このスタンパを用いたプレス工程で行われるのが一般的である。このようなディスク製造業者による再生専用領域へのデータ記録工程において、暗号化メディア鍵データが記録媒体に記録される場合であっても本発明は適用可能である。

【００９１】

（実施の形態３）

本発明の実施の形態３は、実施の形態１と同様、再生専用の記録媒体を用いてコンテンツを配布し、再生装置でコンテンツを再生するシステムに本発明を適用したものである。

【００９２】

以下、本発明の実施の形態３について、図面を参照にしながら説明する。図１３は、コンテンツを暗号化して記録する記録装置１３００及び記録媒体１３２０を示しており、図１４は、記録媒体１３２０から暗号化コンテンツを読み出して復号する第１のカテゴリの再生装置１４００を示しており、図１５は、記録媒体１３２０から暗号化コンテンツを読み出して復号する第２のカテゴリの再生装置１５００を示している。また、図１６は記録媒体１３２０に記録される各種データの具体例を示している。

【００９３】
図１３の記録装置１３００が図１の記録装置１００と異なる点は、第１のカテゴリに対しては第１のメディア鍵を、第２のカテゴリに対しては第２のメディア鍵を、個別に設け、第１及び第２のメディア鍵をそれぞれ第１のメディア鍵暗号化部１３０５及び第２のメディア鍵暗号化部１３０６で暗号化し、コンテンツ鍵を第１及び第２のメディア鍵を用いてそれぞれ第１のコンテンツ鍵暗号化部１３０７及び第２のコンテンツ鍵暗号化部１３０８で暗号化し、記録媒体１３２０に記録するようにしたことである。その他の点は図１の記録装置１００と同じであるので、その説明は省略する。
【００９４】
記録媒体１３２０は、第１のメディア鍵暗号化部１３０５が生成した第１の暗号化メディア鍵データを記録する第１の暗号化メディア鍵データ記録領域１３２１と、第２のメディア鍵暗号化部１３０６が生成した第２の暗号化メディア鍵データを記録する第２の暗号化メディア鍵データ記録領域１３２２と、第１のコンテンツ鍵暗号化部１３０７が生成した第１の暗号化コンテンツ鍵を記録する第１の暗号化コンテンツ鍵記録領域１３２３と、第２のコンテンツ鍵暗号化部１３０８が生成した第２の暗号化コンテンツ鍵を記録する第２の暗号化コンテンツ鍵記録領域１３２４と、コンテンツ暗号化部１３０９が生成した暗号化コンテンツを記録する暗号化コンテンツ記録領域１３２５とを備える。
【００９５】
第１カテゴリの再生装置１４００及び第２のカテゴリの再生装置１５００は、それぞれ記録媒体１３２０から読み出した第１および第２の暗号化コンテンツ鍵を復号してコンテンツ鍵を取得する。その他の点については、実施の形態１における第１のカテゴリの再生装置２００及び第２のカテゴリの再生装置３００と同様であるので、その説明は省略する。
【００９６】
図１６は、ｍ台の第１のカテゴリの再生装置及びｎ台の第２のカテゴリの再生装置がそれぞれ固有のデバイス鍵を１個だけ保有しており、第１のカテゴリの再生装置２と第２のカテゴリの再生装置３が無効化されているとした場合の、記録媒体１３２０に記録される各種データの具体例を示している。図１６中で、第１のカテゴリの再生装置ｉ（ｉ＝１～ｍ）が保有するデバイス鍵をＤＫＡｉ、第２のカテゴリの再生装置ｊ（ｊ＝１～ｎ）が保有するデバイス鍵をＤＫＢｊとしている。また、Ｅａ（Ｘ，Ｙ）、Ｅｂ（Ｘ，Ｙ）、Ｅｃ（Ｘ，Ｙ）、Ｅｄ（Ｘ，Ｙ）及びＥｅ（Ｘ，Ｙ）はデータＹを鍵データＸを用いて暗号化する関数を意味する。なお、使用される暗号アルゴリズムは、公知の技術で実現可能であり、本実施の形態では鍵長５６ｂｉｔのＤＥＳ暗号を使用した。
【００９７】
（第１の暗号化メディア鍵データ記録領域１３２１）
第１の暗号化メディア鍵データ記録領域１３２１には、第１のカテゴリの再生装置が保有するデバイス鍵（ＤＫＡ１～ＤＫＡｍ）で暗号化された第１のメディア鍵（ＭＫ１）が記録されている。ここで、第１のカテゴリの再生装置２は無効化されており、ＤＫＡ２では第１のメディア鍵（ＭＫ１）とはまったく無関係のデータ「０」が暗号化されて記録されている。これは第１の暗号化メディア鍵データを生成する際に、第１のメディア鍵暗号化部１３０５において、第１のカテゴリのうち無効化すべき再生装置の情報として再生装置２が入力され、再生装置２では正しいメディア鍵が得られないように処理された結果である。第１の暗号化メディア鍵データをこのように生成することにより、再生装置２を除く第１のカテゴリの再生装置が正しい第１のメディア鍵（ＭＫ１）を復号することができ、再生装置２をシステムから排除することができる。
【００９８】
（第２の暗号化メディア鍵データ記録領域１３２２）
第２の暗号化メディア鍵データ記録領域１３２２には、第２のカテゴリの再生装置が保有するデバイス鍵（ＤＫＢ１～ＤＫＢｎ）で暗号化された第２のメディア鍵（ＭＫ２）が記録されている。ここで、第２のカテゴリの再生装置３は無効化されており、ＤＫＢ３で

は第２のメディア鍵（ＭＫ２）とはまったく無関係のデータ「０」が暗号化されて記録されている。これは第２の暗号化メディア鍵データを生成する際に、第２のメディア鍵暗号化部１３０６において、第２のカテゴリのうち無効化すべき再生装置の情報として再生装置３が入力され、再生装置３では正しいメディア鍵が得られないように処理された結果である。第２の暗号化メディア鍵データをこのように生成することにより、再生装置３を除く第２のカテゴリの再生装置が正しい第２のメディア鍵（ＭＫ２）を復号することができ、再生装置３をシステムから排除することができる。

【００９９】

（第１の暗号化コンテンツ鍵記録領域１３２３）

第１の暗号化コンテンツ鍵記録領域１３２３には第１のメディア鍵（ＭＫ１）で暗号化されたコンテンツ鍵（ＣＫ）が記録されている。

【０１００】

（第２の暗号化コンテンツ鍵記録領域１３２４）

第２の暗号化コンテンツ鍵データ記録領域１３２４には第２のメディア鍵（ＭＫ２）で暗号化されたコンテンツ鍵（ＣＫ）が記録されている。

【０１０１】

（暗号化コンテンツ記録領域１３２５）

暗号化コンテンツ記録領域１３２５には、コンテンツ鍵（ＣＫ）で暗号化されたコンテンツが記録されている。

【０１０２】

以上のように構成された本発明の実施の形態１において、例えば第１のカテゴリの再生装置に付与したデバイス鍵の多数や、第１の暗号化メディア鍵及び第１の暗号化コンテンツ鍵を復号するアルゴリズムがインターネット上で不正に公開され、第１のカテゴリの再生装置の無効化が機能しなくなったと判断された場合には、第１のカテゴリの再生装置の無効化システムを更新することになる。以下、その具体例を説明する。

【０１０３】

（システム更新の具体例１）

第１のカテゴリの再生装置の無効化が機能しなくなったと判断されて以降、新たに作成する記録媒体１３２０に記録する各種データの具体例１を図１７に示す。図１６との違いは、第１の暗号化メディア鍵データの生成に用いるデバイス鍵をＤＫＡ１～ＤＫＡｍからＤＫＡ’１～ＤＫＡ’ｍに変更したことである。これは、前記した実施の形態１で述べたシステム更新の具体例１と同様であるので、詳細についての説明は省略する。

【０１０４】

ここで、新たなデバイス鍵（ＤＫＡ’１～ＤＫＡ’ｍ）のうちの各デバイス鍵は、システム更新前のデバイス鍵（ＤＫＡ１～ＤＫＡｍ）のどれとも一致しないようになっているので、システム更新前に不正な解析行為により暴露されたデバイス鍵がＤＫＡ２以外に存在したとしても、そのデバイス鍵を使って図１７の記録媒体から読み出した第１の暗号化メディア鍵データを復号してメディア鍵（ＭＫ１）を取得することはできず、コンテンツを再生することはできない。

【０１０５】

なお、上記したシステム更新に際して、第２の暗号化メディア鍵データの生成に用いるデバイス鍵（ＤＫＢ１～ＤＫＢｎ）は変更されていないので、第２のカテゴリに属する再生装置には何らの変更を加える必要がない。

【０１０６】

（システム更新の具体例２）

第１のカテゴリの再生装置の無効化が機能しなくなったと判断されて以降、新たに作成する記録媒体１３２０に記録する各種データの具体例２を図１８に示す。図１６との違いは、第１の暗号化メディア鍵データの生成に用いるデバイス鍵をＤＫＡ１～ＤＫＡｍからＤＫＡ’１～ＤＫＡ’ｍに変更したこと、第１の暗号化メディア鍵データの暗号化アルゴリズムをＥａ（Ｘ，Ｙ）からＥａ’（Ｘ，Ｙ）に変更したこと、第１の暗号化コンテンツ

鍵の暗号化アルゴリズムをＥｃ（Ｘ，Ｙ）からＥｃ’（Ｘ，Ｙ）に変更したことである。ここで、新たなデバイス鍵（ＤＫＡ’１～ＤＫＡ’ｍ）のうちの各デバイス鍵は、システム更新前のデバイス鍵（ＤＫＡ１～ＤＫＡｍ）のどれとも一致しないようになっている。

【０１０７】

一方、無効化されていない第１のカテゴリの各再生装置１４００には、新たなデバイス鍵を付与されデバイス鍵格納部１４０１に格納される。メディア鍵復号部１４０２には、以前から組み込まれている図１６の第１の暗号化メディア鍵を復号するための復号アルゴリズムＤａ（Ｘ，Ｙ）に加えて、図１８の第１の暗号化メディア鍵を復号するための復号アルゴリズムＤａ’（Ｘ，Ｙ）が組み込まれる。また、コンテンツ鍵復号部１４０３には、以前から組み込まれている図１６の第１の暗号化コンテンツ鍵を復号するための復号アルゴリズムＤｃ（Ｘ，Ｙ）に加えて、図１８の第１の暗号化コンテンツ鍵を復号するための復号アルゴリズムＤｃ’（Ｘ，Ｙ）が組み込まれる。例えば、第１のカテゴリの再生装置ｍは、以前から保有していたデバイス鍵（ＤＫＡｍ）に加え、新たに付与されたデバイス鍵（ＤＫＡ’ｍ）を保有する。再生装置ｍは、図１６の記録媒体を再生する際には、デバイス鍵ＤＫＡｍと暗号化アルゴリズムＤａ（Ｘ，Ｙ）を用いて、第１の暗号化メディア鍵データを復号して第１のメディア鍵（ＭＫ１）を取得し、取得した第１のメディア鍵（ＭＫ１）と暗号化アルゴリズムＤｃ（Ｘ，Ｙ）を用いて第１の暗号化コンテンツ鍵を復号してコンテンツ鍵（ＣＫ）を取得し、取得したコンテンツ鍵（ＣＫ）を用いて暗号化コンテンツを復号する。一方、図１８の記録媒体を再生する際には、デバイス鍵ＤＫＡ’ｍと暗号アルゴリズムＤａ’（Ｘ，Ｙ）を用いて、第１の暗号化メディア鍵データを復号してメディア鍵（ＭＫ１）を取得し、取得したメディア鍵（ＭＫ１）と暗号化アルゴリズムＤｃ’（Ｘ，Ｙ）を用いて第１の暗号化コンテンツ鍵を復号してコンテンツ鍵（ＣＫ）を取得し、取得したコンテンツ鍵（ＣＫ）を用いて暗号化コンテンツを復号する。本実施の形態ではＥａ（Ｘ，Ｙ）、Ｄａ（Ｘ，Ｙ）、Ｅｃ（Ｘ，Ｙ）及びＤｃ（Ｘ，Ｙ）は鍵長５６ｂｉｔのＤＥＳ暗号を用いたのに対して、Ｅａ’（Ｘ，Ｙ）、Ｄａ’（Ｘ，Ｙ）、Ｅｃ’（Ｘ，Ｙ）及びＤｃ’（Ｘ，Ｙ）、では２キートリプルＤＥＳと呼ばれる鍵長１１２ｂｉｔの暗号を用いた。

【０１０８】

ここで、新たなデバイス鍵（ＤＫＡ’１～ＤＫＡ’ｍ）のうちの各デバイス鍵は、システム更新前のデバイス鍵（ＤＫＡ１～ＤＫＡｍ）のどれとも一致しないようになっているので、システム更新前に不正な解析行為により暴露されたデバイス鍵がＤＫＡ２以外に存在したとしても、そのデバイス鍵を使って図１８の記録媒体から読み出した第１の暗号化メディア鍵データを復号してメディア鍵（ＭＫ１）を取得することはできず、コンテンツを再生することはできない。

【０１０９】

また、デバイス鍵の鍵長や暗号アルゴリズムを変更して暗号強度の高いものにすることができるので、システムを解析してデバイス鍵を不正取得するといった行為を困難にすることができる。

【０１１０】

なお、上記したシステム更新に際して、第２の暗号化メディア鍵データの生成に用いるデバイス鍵（ＤＫＢ１～ＤＫＢｎ）、第２の暗号化メディア鍵データの暗号化アルゴリズム、及び第２の暗号化コンテンツ鍵データの暗号化アルゴリズムは変更されていないので、第２のカテゴリに属する再生装置には何らの変更を加える必要がない。

【０１１１】

以上のように構成された本発明の実施の形態３によれば、第１のカテゴリの再生装置１４００及び第２のカテゴリの再生装置１５００は、それぞれ異なるカテゴリの再生装置を無効化するための第１もしくは第２の暗号化メディア鍵データを読み込む必要がないため、装置内に設けるメモリ容量を小さくでき、処理時間も短くできる。また、第１の暗号化メディア鍵データ及び第１の暗号化コンテンツ鍵の生成に用いる暗号化アルゴリズムを、それぞれ第２の暗号化メディア鍵データ及び第２の暗号化コンテンツ鍵の生成に用いる暗

号化アルゴリズムと異なるものとすることができるため、第１のカテゴリの再生装置の無効化システムが暴露されるような事態に陥った場合にも、第１のカテゴリの再生装置に付与するデバイス鍵の鍵長や第１の暗号化メディア鍵データの生成アルゴリズムを変更することで、第２のカテゴリの再生装置に影響を与えることなく、無効化システムを変更することが可能になる。

【０１１２】

また、本実施の形態では第１のカテゴリと第２のカテゴリに対して個別にメディア鍵を設け、それぞれを用いた暗号化コンテンツ鍵の階層を設けることにより、カテゴリ間の独立性を高めることが可能となる。すなわち第１のカテゴリに属する再生装置からデバイス鍵が暴露された場合であっても、それを用いて得られるメディア鍵は第１のメディア鍵のみであり、第２のメディア鍵が暴露されることを防ぐことが可能となる。これは、本実施の形態のように第１のカテゴリは復号アルゴリズムや鍵の更新や追加が容易ではあるが堅牢な実装が困難なソフトウェアで実装される再生装置とし、第２のカテゴリは堅牢ではあるが復号アルゴリズムや鍵の更新や追加が困難なハードウェアで実装される再生装置とした場合に、特に有効である。

【０１１３】

なお、図１３では、第１のメディア鍵、第２のメディア鍵及びコンテンツ鍵が記録装置１３００の外部から入力される形態としたが、本発明はその構成に限定されるものではない。例えば、記録装置１３００が第１のメディア鍵、第２のメディア鍵及びコンテンツ鍵を格納する格納部を有する構成であってもよい。また、記録装置１３００が第１のメディア鍵、第２のメディア鍵及びコンテンツ鍵をその都度生成する生成部を有する構成であってもよい。

【０１１４】

また、図１３では、コンテンツをコンテンツ鍵で暗号化し、コンテンツ鍵を第１及び第２のメディア鍵で暗号化する２階層の構成としたが、本発明はそれに限定されるものではない。例えば、鍵を追加して暗号化の階層をさらに増やす構成であってもよい。

【０１１５】

また、本実施の形態では記録装置として図１３に示すように、各カテゴリのデバイス鍵格納部、メディア鍵暗号化部、コンテンツ鍵暗号化部、コンテンツ暗号化部及び記録媒体への各データのの記録が一体の構成としたが、本発明はそれに限定されるものではい。例えば、各カテゴリのデバイス鍵格納部、メディア鍵暗号化部、コンテンツ鍵暗号化部（図１３中の破線で囲んだ部分）は、その管理、運用に高い秘匿性が要求されることから、システム全体の鍵管理や再生装置に対する鍵発行等を運用する機関に設置される装置に内蔵され、コンテンツ暗号部や記録媒体への各データの記録はコンテンツ製造機関や記録媒体製造機関に設置される装置で実行される形態であっても良い。

【０１１６】

また、本実施の形態ではシステム更新において第１の暗号化メディア鍵データを生成する際に、図１７のＥａ（ＤＫＡ’２，０）や図１８のＥａ’（ＤＫＡ’２，０）のようにシステム更新の時点で無効化されている再生装置にもデータを割り当てる構成としているが、無効化されている再生装置にはデータを割り当てない構成とすることも可能である。その場合、無効化されていない再生装置の使うべき暗号化メディア鍵の位置も更新し、新たなデバイス鍵を付与する際に新たな位置情報も付与することで、システム更新の前後において暗号化メディア鍵の位置が変わったとしても無効化されていない再生装置は適切なデータを用いることができ、正しいメディア鍵を得ることができる。こうした場合、システム更新後の第１の暗号化メディア鍵データ記録領域に格納すべきデータの容量を削減することができる。あるいは容量の最大値が限定されている場合は新たに第１のカテゴリに属する再生装置の台数を増やすことが可能となる。

【０１１７】

また、本実施の形態では、図１６に示すような暗号化メディア鍵データを用いて再生装置の無効化を行う方法としたが、無効化の方法は他の方法を利用してもよく、例えば特許

文献１として開示されている木構造を利用した無効化方法を用いても良い。

【０１１８】

また、本実施の形態では、暗号アルゴリズムとして鍵長５６ｂｉｔのＤＥＳ、あるいはシステム更新後の暗号アルゴリズムとして鍵長１１２ｂｉｔの２キートリプルＤＥＳを用いたが、本発明はこれに限定されるものではなく、他の暗号アルゴリズム、例えば次世代の標準暗号とされる鍵長１２８ｂｉｔのＡＥＳ等を用いても良い。

【０１１９】

なお、本実施の形態は、再生専用の記録媒体を用いてコンテンツを配布し、再生装置でコンテンツを再生するシステムに本発明を適用したものであるが、本発明はそれに限定されるものではない。前記した実施の形態２のように、鍵生成装置で各カテゴリ用の暗号化メディア鍵データ及び暗号化コンテンツ鍵を生成して記録媒体に記録し、記録装置で暗号化メディア鍵データ及び暗号化コンテンツ鍵を復号してコンテンツを暗号化する構成とすることにより、書き換え型もしくは追記型の記録媒体を用いるシステムにも適用することができる。

【０１２０】

（実施の形態４）

本発明の実施の形態４は、実施の形態１と同様、再生専用の記録媒体を用いてコンテンツを配布し、再生装置でコンテンツを再生するシステムに本発明を適用したものである。

【０１２１】

以下、本発明の実施の形態４について、図面を参照にしながら説明する。図１９は、コンテンツを暗号化して記録する記録装置１９００及び記録媒体１９２０を示しており、図２０は、記録媒体１９２０から暗号化コンテンツを読み出して復号する第１の再生装置２０００を示しており、図２１は、記録媒体１９２０から暗号化コンテンツを読み出して復号する第２の再生装置２１００を示している。また、図２２は記録媒体１９２０に記録される各種データの具体例を示している。

【０１２２】

図１９の記録装置１９００が図１の記録装置１００と異なる点は、コンテンツに対して第１のコンテンツ鍵を用いて第１のコンテンツ暗号化部１９０９で第１のコンテンツ暗号化を施し、その出力に対して第２のコンテンツ鍵を用いて第２のコンテンツ暗号化部１９１０で第２のコンテンツ暗号化を施し、メディア鍵を用いて第１及び第２のコンテンツ鍵をそれぞれ第１のコンテンツ鍵暗号化部１９０７及び第２のコンテンツ鍵暗号化部１９０８で暗号化し、記録媒体１９２０に記録するようにしたことである。その他の点は図１の記録装置１００と同じであるので、その説明は省略する。

【０１２３】

記録媒体１９２０は、第１の暗号化メディア鍵データを記録する第１の暗号化メディア鍵データ記録領域１９２１と、第２の暗号化メディア鍵データを記録する第２の暗号化メディア鍵データ記録領域１９２２と、第１のコンテンツ鍵暗号化部１９０７が生成した第１の暗号化コンテンツ鍵を記録する第１の暗号化コンテンツ鍵記録領域１９２３と、第２のコンテンツ鍵暗号化部１９０８が生成した第２の暗号化コンテンツ鍵を記録する第２の暗号化コンテンツ鍵記録領域１９２４と、第２のコンテンツ暗号化部１９１０が生成した暗号化コンテンツを記録する暗号化コンテンツ記録領域１９２５とを備える。

【０１２４】

第１の再生装置２０００は、読み出し装置２０１０及び復号装置２０２０とから構成される。

【０１２５】

読み出し装置２０１０は、デバイス鍵を秘密に保有するデバイス鍵格納部２０１１と、デバイス鍵を用いて記録媒体１９２０から読み出した第２の暗号化メディア鍵データを復号してメディア鍵を取得する第２のメディア鍵復号部２０１２と、取得したメディア鍵を用いて記録媒体から読み出した第２の暗号化コンテンツ鍵を復号してコンテンツ鍵を取得する第２のコンテンツ鍵復号部２０１３と、取得したコンテンツ鍵を用いて記録媒体１９

２０から読み出した暗号化コンテンツに第２のコンテンツ復号処理を施す第２のコンテンツ復号部２０１４とを備え、第２のコンテンツ復号部２０１４で暗号化コンテンツに第２の復号処理を施した結果の中間データを記録媒体１９２０から読み出した第１の暗号化メディア鍵データ及び第１の暗号化コンテンツ鍵とともに復号装置２０２０に供給する。本実施の形態において、読み出し装置２０１０は上記した構成要素がハードウェアで実装されており、第２のカテゴリに属するものとした。

【０１２６】

復号装置２０２０は、デバイス鍵を秘密に保有するデバイス鍵格納部２０２１と、デバイス鍵を用いて読み出し装置２０１０から供給される第１の暗号化メディア鍵データを復号してメディア鍵を取得する第１のメディア鍵復号部２０２２と、取得したメディア鍵を用いて読み出し装置２０１０から供給される第１の暗号化コンテンツ鍵を復号して第１のコンテンツ鍵を取得する第１のコンテンツ鍵復号部２０２３と、取得した第１のコンテンツ鍵を用いて読み取り装置２０１０から供給される中間データに第１のコンテンツ復号処理を施してコンテンツを取得する第１のコンテンツ復号部２０２４とを備える。本実施の形態において、復号装置２０２０は上記した構成要素がソフトウェアで実装されており、第１のカテゴリに属するものとした。

【０１２７】

第２の再生装置２１００は、第２のカテゴリの再生装置であり、デバイス鍵を秘密に保有するデバイス鍵格納部２１０１と、デバイス鍵を用いて記録媒体１９２０から読み出した第２の暗号化メディア鍵データを復号してメディア鍵を取得するメディア鍵復号部２１０２と、取得したメディア鍵を用いて記録媒体から読み出した第２の暗号化コンテンツ鍵を復号して第２のコンテンツ鍵を取得する第２のコンテンツ鍵復号部２１０３と、取得した第２のコンテンツ鍵を用いて記録媒体１９２０から読み出した暗号化コンテンツに第２のコンテンツ復号処理を施す第２のコンテンツ復号部２１０４と、取得したメディア鍵を用いて記録媒体から読み出した第１の暗号化コンテンツ鍵データを復号して第１のコンテンツ鍵を取得する第１のコンテンツ鍵復号部２１０５と、第２のコンテンツ復号部２１０４の出力に第１のコンテンツ鍵を用いて第１のコンテンツ復号処理を施してコンテンツを取得する第１のコンテンツ復号部２１０６とを備える。本実施の形態において、第２の再生装置２１００は、上記した構成要素がハードウェアで実装されており、第２のカテゴリに属するものとした。

【０１２８】

本実施の形態ではパソコン上のアプリケーションプログラムのようにソフトウェアで実装される復号装置を第１のカテゴリに属する復号装置とし、一般的な民生プレーヤ及びパソコンに接続もしくは内蔵される光ディスクドライブのようにハードウェアで実装される装置を第２のカテゴリに属する装置とした。

【０１２９】

図２２は、ｍ台の第１のカテゴリの復号装置及びｎ台の第２のカテゴリの装置がそれぞれ固有のデバイス鍵を１個だけ保有しており、第１のカテゴリの復号装置２と第２のカテゴリの装置３が無効化されているとした場合の、記録媒体１９２０に記録される各種データの具体例を示している。図２２中で、第１のカテゴリの復号装置ｉ（ｉ＝１～ｍ）が保有するデバイス鍵をＤＫＡｉ、第２のカテゴリの装置ｊ（ｊ＝１～ｎ）が保有するデバイス鍵をＤＫＡｊとしている。また、Ｅａ（Ｘ，Ｙ）、Ｅｂ（Ｘ，Ｙ）、Ｅｃ（Ｘ，Ｙ）、Ｅｄ（Ｘ，Ｙ）、Ｅｅ（Ｘ，Ｙ）及びＥｆ（Ｘ，Ｙ）はデータＹを鍵データＸを用いて暗号化する関数を意味する。なお、使用される暗号アルゴリズムは公知の技術で実現可能であり、本実施の形態では鍵長５６ビットのＤＥＳ暗号を使用した。

【０１３０】

第１の暗号化メディア鍵データ記録領域１９２１及び第２の暗号化メディア鍵データ記録領域１９２２に記録されるデータは、それぞれ、前記した実施の形態１における第１の暗号化メディア鍵データ記録領域１２１及び第２の暗号化メディア鍵データ記録領域１２２に記録されるデータと同じであるので、その説明は省略する。

【０１３１】
（第１の暗号化コンテンツ鍵記録領域１９２３）
第１の暗号化コンテンツ鍵記録領域１９２３にはメディア鍵（ＭＫ）で暗号化された第１のコンテンツ鍵（ＣＫ１）が記録されている。
【０１３２】
（第２の暗号化コンテンツ鍵記録領域１９２４）
第２の暗号化コンテンツ鍵記録領域１９２４にはメディア鍵（ＭＫ）で暗号化された第２のコンテンツ鍵（ＣＫ２）が記録されている。
【０１３３】
（暗号化コンテンツ記録領域１９２５）
暗号化コンテンツ記録領域１９２５には、第１のコンテンツ鍵（ＣＫ１）及び第２のコンテンツ鍵（ＣＫ２）で暗号化されたコンテンツが記録されている。
【０１３４】
以上のように構成された本発明の実施の形態４において、例えば第１のカテゴリの復号装置に付与したデバイス鍵の多数や、第１の暗号化メディア鍵データを復号するアルゴリズムがインターネット上で不正に公開され、第１のカテゴリの復号装置の無効化が機能しなくなったと判断された場合には、第１のカテゴリの復号装置の無効化システムを更新することになる。以下、その具体例を説明する。
【０１３５】
（システム更新の具体例１）
第１のカテゴリの復号装置の無効化が機能しなくなったと判断されて以降、新たに作成する記録媒体１９２０に記録する各種データの具体例１を図２３に示す。図２２との違いは、第１の暗号化メディア鍵の生成に用いるデバイス鍵をＤＫＡ１～ＤＫＡｍからＤＫＡ’１～ＤＫＡ’ｍに変更したことである。これは、前記した実施の形態１で述べたシステム更新の具体例１と同様であるので、詳細についての説明は省略する。
【０１３６】
ここで、新たなデバイス鍵（ＤＫＡ’１～ＤＫＡ’ｍ）のうちの各デバイス鍵は、システム更新前のデバイス鍵（ＤＫＡ１～ＤＫＡｍ）のどれとも一致しないようになっているので、システム更新前に不正な解析行為により暴露されたデバイス鍵がＤＫＡ２以外に存在したとしても、そのデバイス鍵を使って図２３の記録媒体から読み出した第１の暗号化メディア鍵データを復号してメディア鍵（ＭＫ）を取得することはできず、コンテンツを再生することはできない。
【０１３７】
なお、上記したシステム更新に際して、第２の暗号化メディア鍵データの生成に用いるデバイス鍵（ＤＫＢ１～ＤＫＢｎ）は変更されていないので、第２のカテゴリに属する装置には何らの変更を加える必要がない。
【０１３８】
（システム更新の具体例２）
第１のカテゴリの復号装置の無効化が機能しなくなったと判断されて以降、新たに作成する記録媒体１９２０に記録する各種データの具体例２を図２４に示す。図２２との違いは、第１の暗号化メディア鍵データの生成に用いるデバイス鍵をＤＫＡ１～ＤＫＡｍからＤＫＡ’１～ＤＫＡ’ｍに変更したことと、暗号化アルゴリズムをＥａ（Ｘ，Ｙ）からＥａ’（Ｘ，Ｙ）に変更したことである。これは、前記した実施の形態１で述べたシステム更新の具体例２と同様であるので、詳細についての説明は省略する。
【０１３９】
ここで、新たなデバイス鍵（ＤＫＡ’１～ＤＫＡ’ｍ）のうちの各デバイス鍵は、システム更新前のデバイス鍵（ＤＫＡ１～ＤＫＡｍ）のどれとも一致しないようになっているので、システム更新前に不正な解析行為により暴露されたデバイス鍵がＤＫＡ２以外に存在したとしても、そのデバイス鍵を使って図２４の記録媒体から読み出した第１の暗号化メディア鍵データを復号してメディア鍵（ＭＫ）を取得することはできず、コンテンツを

再生することはできない。

【０１４０】

また、デバイス鍵の鍵長や暗号アルゴリズムを変更して暗号強度の高いものにすることができるので、システムを解析してデバイス鍵を不正取得するといった行為を困難にすることができる。

【０１４１】

なお、上記したシステム更新に際して、第２の暗号化メディア鍵データの生成に用いるデバイス鍵（ＤＫＢ１～ＤＫＢｎ）及び第２の暗号化メディア鍵データの暗号化アルゴリズムは変更されていないので、第２のカテゴリに属する装置には何らの変更を加える必要がない。

【０１４２】

以上のように構成された本発明の実施の形態４によれば、第１のカテゴリの装置（復号装置２０２０）及び第２のカテゴリの装置（読み出し装置２０１０及び第２の再生装置２１００）は、それぞれ異なるカテゴリの装置を無効化するための第１もしくは第２の暗号化メディア鍵データを読み込む必要がないため、装置内に設けるメモリ容量を小さくでき、処理時間も短くできる。また、第１の暗号化メディア鍵データの生成に用いる暗号化アルゴリズムを第２の暗号化メディア鍵データの生成に用いる暗号化アルゴリズムと異なるものとすることができるため、第１のカテゴリの復号装置の無効化システムが暴露されるような事態に陥った場合にも、第１のカテゴリの復号装置に付与するデバイス鍵の鍵長や第１の暗号化メディア鍵データの生成アルゴリズムを変更することで、第２のカテゴリの装置に影響を与えることなく、無効化システムを変更することが可能になる。さらに、第１のカテゴリの復号装置２０２０には、第２の暗号化コンテンツ鍵を復号するためのアルゴリズムは実装されていないので、第１のカテゴリの復号装置の何れかを解析して保有するデバイス鍵や復号アルゴリズムを暴露したとしても、コンテンツの復号に必要な全ての情報を取得することはできず、より堅牢な著作権保護システムを構築できる。これは、本実施の形態のように第１のカテゴリは復号アルゴリズムや鍵の更新や追加が容易ではあるが堅牢な実装が困難なソフトウェアで実装される復号装置とし、第２のカテゴリは堅牢ではあるが復号アルゴリズムや鍵の更新や追加が困難なハードウェアで実装される再生装置もしくは読み取り装置とした場合に、特に有効である。

【０１４３】

なお、図１９で、メディア鍵、第１のコンテンツ鍵、及び第２のコンテンツ鍵が記録装置１９００の外部から入力される形態としたが、本発明はその構成に限定されるものではない。例えば、記録装置１９００がメディア鍵、第１のコンテンツ鍵、及び第２のコンテンツ鍵を格納する格納部を有する構成であってもよい。また、記録装置１９００がメディア鍵、第１のコンテンツ鍵、及び第２のコンテンツ鍵をその都度生成する生成部を有する構成であってもよい。

【０１４４】

また、図１９では、コンテンツを第１及び第２のコンテンツ鍵で暗号化し、第１及び第２のコンテンツ鍵をメディア鍵で暗号化する２階層の構成としたが、本発明はそれに限定されるものではない。例えば、鍵を追加して暗号化の階層をさらに増やす構成であってもよい。

【０１４５】

また、本実施の形態では記録装置として図１９に示すように、各カテゴリのデバイス鍵格納部、メディア鍵暗号化部、コンテンツ鍵暗号化部、コンテンツ暗号化部及び記録媒体への各データの記録が一体の構成としたが、本発明はそれに限定されるものではなく、記録装置が分離して構成されるものであっても良い。例えば、各カテゴリのデバイス鍵格納部、メディア鍵暗号化部、及びコンテンツ鍵暗号化部（図１９中の破線で囲んだ部分）は、その管理、運用に高い秘匿性が要求されることから、システム全体の鍵管理や再生装置に対する鍵発行等を運用する機関に設置される装置に内蔵され、コンテンツ暗号部や記録媒体に各データへの記録はコンテンツ製造機関や記録媒体製造機関に設置される装置で実

行される形態であっても良い。

【０１４６】

また、本実施の形態ではシステム更新において第１の暗号化メディア鍵データを生成する際に、図２３のＥａ（ＤＫＡ’２，０）や図２４のＥａ’（ＤＫＡ’２，０）のようにシステム更新の時点で無効化されている復号装置にもデータを割り当てる構成としているが、無効化されている復号装置にはデータを割り当てない構成とすることも可能である。その場合、無効化されていない復号装置の使うべき暗号化メディア鍵の位置も更新し、新たなデバイス鍵を付与する際に新たな位置情報も付与することで、システム更新の前後において暗号化メディア鍵の位置が変わったとしても無効化されていない復号装置は適切なデータを用いることができ、正しいメディア鍵を得ることができる。こうした場合、システム更新後の第１の暗号化メディア鍵データ記録領域に格納すべきデータの容量を削減することができる。あるいは容量の最大値が限定されている場合は新たに第１のカテゴリに属する復号装置の台数を増やすことが可能となる。

【０１４７】

また、本実施の形態では、図２２に示すような暗号化メディア鍵データを用いて復号装置の無効化を行う方法としたが、無効化の方法は他の方法を利用してもよく、例えば特許文献１として開示されている木構造を利用した無効化方法を用いても良い。

【０１４８】

また、本実施の形態では、暗号アルゴリズムとして鍵長５６ｂｉｔのＤＥＳ、あるいはシステム更新後の暗号アルゴリズムとして鍵長１１２ｂｉｔの２キートリプルＤＥＳを用いたが、本発明はこれに限定されるものではなく、他の暗号アルゴリズム、例えば次世代の標準暗号とされる鍵長１２８ｂｉｔのＡＥＳ等を用いても良い。

【０１４９】

また、図２２では、コンテンツ全体を第１のコンテンツ鍵（ＣＫ１）で暗号化した後、さらに第２のコンテンツ鍵（ＣＫ２）で暗号化するようにしたが、本発明はそれに限定されるものではない。例えば、コンテンツを複数のブロックに分割したうちのいくつかのブロックを第１のコンテンツ鍵（ＣＫ１）で暗号化し、他のブロックを第２のコンテンツ鍵（ＣＫ２）で暗号化するようにしてもよい。

【０１５０】

なお、本実施の形態は、再生専用の記録媒体を用いてコンテンツを配布し、再生装置でコンテンツを再生するシステムに本発明を適用したものであるが、本発明はそれに限定されるものではない。前記した実施の形態２のように、鍵生成装置で各カテゴリ用の暗号化メディア鍵データ及び暗号化コンテンツ鍵を生成して記録媒体に記録し、記録装置で暗号化メディア鍵データ及び暗号化コンテンツ鍵を復号してコンテンツを暗号化する構成とすることにより、書き換え型もしくは追記型の記録媒体を用いるシステムにも適用することができる。

【０１５１】

（実施の形態５）

本発明の実施の形態５は、実施の形態４のシステムにおいて、第１のカテゴリと第２のカテゴリに対して個別にメディア鍵を設け、それぞれを用いた第１の暗号化コンテンツ鍵の階層を設けるようにしたものである。

【０１５２】

以下、本発明の実施の形態５について、図面を参照にしながら説明する。図２５は、コンテンツを暗号化して記録する記録装置２５００及び記録媒体２５２０を示しており、図２６は、記録媒体２５２０から暗号化コンテンツを読み出して復号する第１の再生装置２６００を示しており、図２７は、記録媒体２５２０から暗号化コンテンツを読み出して復号する第２の再生装置２７００を示している。また、図２８は記録媒体２５２０に記録される各種データの具体例を示している。

【０１５３】

図２５の記録装置２５００が図１９の記録装置１９００と異なる点は、第１のカテゴリ

に対しては第１のメディア鍵を、第２のカテゴリに対しては第２のメディア鍵を、個別に設け、第１及び第２のメディア鍵をそれぞれ第１のメディア鍵暗号化部２５０５及び第２のメディア鍵暗号化部２５０６で暗号化し、第１のコンテンツ鍵を第１及び第２のメディア鍵を用いてそれぞれ第１コンテンツ鍵暗号化部（１）２５０７及び第１のコンテンツ鍵暗号化部（２）２５１１で暗号化し、記録媒体２５２０に記録するようにしたことである。その他の点については、前記した実施の形態４の記録装置１９００と同じであるので、その説明は省略する。

【０１５４】

記録媒体２５２０は、第１の暗号化メディア鍵データを記録する第１の暗号化メディア鍵データ記録領域２５２１と、第２の暗号化メディア鍵データを記録する第２の暗号化メディア鍵データ記録領域２５２２と、第１のコンテンツ鍵暗号化部（１）２５０７が生成した第１の暗号化コンテンツ鍵（１）を記録する第１の暗号化コンテンツ鍵（１）記録領域２５２３と、第１のコンテンツ鍵暗号化部（２）２５１１が生成した第１の暗号化コンテンツ鍵（２）を記録する第１の暗号化コンテンツ鍵（２）記録領域２５２６と、第２の暗号化コンテンツ鍵を記録する第２の暗号化コンテンツ鍵記録領域２５２４と、暗号化コンテンツを記録する暗号化コンテンツ記録領域２５２５とを備える。

【０１５５】

第１の再生装置２６００において復号装置２６２０は、読み出し装置２６１０が記録媒体２５２０から読み出した第１の暗号化コンテンツ鍵（１）を復号して第１のコンテンツ鍵を取得する。その他の点については、前記した実施の形態４における第１の再生装置２０００と同様であるので、その説明は省略する。

【０１５６】

第２の再生装置２７００は、記録媒体２５２０から読み出した第１の暗号化コンテンツ鍵（２）を復号して第１のコンテンツ鍵を取得する。その他の点については、前記した実施の形態４における第２の再生装置２１００と同様であるので、その説明は省略する。

【０１５７】

図２８は、記録媒体２５２０に記録される各種データの具体例を示している。第１の暗号化メディア鍵データ記録領域２５２１には、第１のカテゴリの復号装置が保有するデバイス鍵（ＤＫＡ１～ＤＫＡｍ）で暗号化された第１のメディア鍵（ＭＫ１）が記録されており、第２の暗号化メディア鍵データ記録領域２５２２には、第２のカテゴリの装置が保有するデバイス鍵（ＤＫＢ１～ＤＫＢｍ）で暗号化された第２のメディア鍵（ＭＫ２）がきろくされている。また、第１の暗号化コンテンツ鍵（１）記録領域２５２３には、第１のメディア鍵（ＭＫ１）で暗号化された第１のコンテンツ鍵（ＣＫ１）が記録されており、第１の暗号化コンテンツ鍵（２）記録領域２５２６には、第２のメディア鍵（ＭＫ２）で暗号化された第１のコンテンツ鍵（ＣＫ１）が記録されている。その他の点については、前記した図２２と同じであるので、説明を省略する。なお、図２８中の、Ｅｇ（Ｘ，Ｙ）はデータＹを鍵データＸを用いて暗号化する関数を意味し、本実施の形態では鍵長５６ビットのＤＥＳ暗号を使用した。

【０１５８】

以上のように構成された本発明の実施の形態５において、例えば第１のカテゴリの復号装置に付与したデバイス鍵の多数や、第１の暗号化メディア鍵を復号するアルゴリズムがインターネット上で不正に公開され、第１のカテゴリの復号装置の無効化が機能しなくなったと判断された場合には、第１のカテゴリの復号装置の無効化システムを更新することになる。以下、その具体例を説明する。

【０１５９】

（システム更新の具体例１）

第１のカテゴリの復号装置の無効化が機能しなくなったと判断されて以降、新たに作成する記録媒体２５２０に記録する各種データの具体例１を図２９に示す。図２８との違いは、第１の暗号化メディア鍵データの生成に用いるデバイス鍵をＤＫＡ１～ＤＫＡｍからＤＫＡ’１～ＤＫＡ’ｍに変更したことである。これは、前記した実施の形態１で述べ

たシステム更新の具体例１と同様であるので、詳細についての説明は省略する。

【０１６０】

（システム更新の具体例２）

第１のカテゴリの復号装置の無効化が機能しなくなったと判断されて以降、新たに作成する記録媒体２５２０に記録する各種データの具体例２を図３０に示す。図２２との違いは、第１の暗号化メディア鍵データの生成に用いるデバイス鍵をＤＫＡ１～ＤＫＡｍからＤＫＡ’１～ＤＫＡ’ｍに変更したこと、暗号化アルゴリズムをＥａ（Ｘ，Ｙ）からＥａ’（Ｘ，Ｙ）に変更したこと、及び第１の暗号化コンテンツ鍵（１）の暗号化アルゴリズムをＥｃ（Ｘ，Ｙ）からＥｃ’（Ｘ，Ｙ）に変更したことである。これは、前記した実施の形態３で述べたシステム更新の具体例２と同様であるので、詳細についての説明は省略する。

【０１６１】

以上のように構成された本発明の実施の形態５によれば、前記した実施の形態４同様に、堅牢な著作権保護システムを構築できる。さらに、本実施の形態では第１のカテゴリと第２のカテゴリに対して個別にメディア鍵を設け、それぞれを用いた暗号化コンテンツ鍵の階層を設けることにより、カテゴリ間の独立性を高めることが可能となる。すなわち第１のカテゴリに属する装置からデバイス鍵が暴露された場合であっても、それを用いて得られるメディア鍵は第１のメディア鍵のみであり、第２のメディア鍵が暴露されることを防ぐことが可能となる。これは、本実施の形態のように第１のカテゴリは復号アルゴリズムや鍵の更新や追加が容易ではあるが堅牢な実装が困難なソフトウェアで実装される復号装置とし、第２のカテゴリは堅牢ではあるが復号アルゴリズムや鍵の更新や追加が困難なハードウェアで実装される再生装置もしくは読み取り装置とした場合に、特に有効である。

【０１６２】

なお、図２５で、第１のメディア鍵、第２のメディア鍵、第１のコンテンツ鍵、及び第２のコンテンツ鍵が記録装置２５００の外部から入力される形態としたが、本発明はその構成に限定されるものではない。例えば、記録装置２５００がこれらの鍵を格納する格納部を有する構成であってもよい。また、記録装置２５００がこれらの鍵をその都度生成する生成部を有する構成であってもよい。

【０１６３】

また、図２５では、コンテンツを第１及び第２のコンテンツ鍵で暗号化し、第１及び第２のコンテンツ鍵をメディア鍵で暗号化する構成としたが、本発明はそれに限定されるものではない。例えば、鍵を追加して暗号化の階層をさらに増やす構成であってもよい。

【０１６４】

また、本実施の形態では記録装置として図２５に示すように、各カテゴリのデバイス鍵格納部、メディア鍵暗号化部、コンテンツ鍵暗号化部、コンテンツ暗号化部及び記録媒体への各データの記録が一体の構成としたが、本発明はそれに限定されるものではなく、記録装置が分離して構成されるものであっても良い。例えば、各カテゴリのデバイス鍵格納部、メディア鍵暗号化部、及びコンテンツ鍵暗号化部（図２５中の破線で囲んだ部分）は、その管理、運用に高い秘匿性が要求されることから、システム全体の鍵管理や再生装置に対する鍵発行等を運用する機関に設置される装置に内蔵され、コンテンツ暗号部や記録媒体に各データへの記録はコンテンツ製造機関や記録媒体製造機関に設置される装置で実行される形態であっても良い。

【０１６５】

また、本実施の形態ではシステム更新において第１の暗号化メディア鍵データを生成する際に、図２９のＥａ（ＤＫＡ’２，０）や図３０のＥａ’（ＤＫＡ’２，０）のようにシステム更新の時点で無効化されている復号装置にもデータを割り当てる構成としているが、無効化されている復号装置にはデータを割り当てない構成とすることも可能である。その場合、無効化されていない復号装置の使うべき暗号化メディア鍵の位置も更新し、新たなデバイス鍵を付与する際に新たな位置情報も付与することで、システム更新の前後に

おいて暗号化メディア鍵の位置が変わったとしても無効化されていない復号装置は適切なデータを用いることができ、正しいメディア鍵を得ることができる。こうした場合、システム更新後の第１の暗号化メディア鍵データ記録領域に格納すべきデータの容量を削減することができる。あるいは容量の最大値が限定されている場合は新たに第１のカテゴリに属する復号装置の台数を増やすことが可能となる。

【０１６６】

また、本実施の形態では、図２８に示すような暗号化メディア鍵データを用いて復号装置の無効化を行う方法としたが、無効化の方法は他の方法を利用してもよく、例えば特許文献１として開示されている木構造を利用した無効化方法を用いても良い。

【０１６７】

また、本実施の形態では、暗号アルゴリズムとして鍵長５６ｂｉｔのＤＥＳ、あるいはシステム更新後の暗号アルゴリズムとして鍵長１１２ｂｉｔの２キートリプルＤＥＳを用いたが、本発明はこれに限定されるものではなく、他の暗号アルゴリズム、例えば次世代の標準暗号とされる鍵長１２８ｂｉｔのＡＥＳ等を用いても良い。

【０１６８】

また、図２８では、コンテンツ全体を第１のコンテンツ鍵（ＣＫ１）で暗号化した後、さらに第２のコンテンツ鍵（ＣＫ２）で暗号化するようにしたが、本発明はそれに限定されるものではない。例えば、コンテンツを複数のブロックに分割したうちのいくつかのブロックを第１のコンテンツ鍵（ＣＫ１）で暗号化し、他のブロックを第２のコンテンツ鍵（ＣＫ２）で暗号化するようにしてもよい。

【０１６９】

なお、本実施の形態は、再生専用の記録媒体を用いてコンテンツを配布し、再生装置でコンテンツを再生するシステムに本発明を適用したものであるが、本発明はそれに限定されるものではない。前記した実施の形態２のように、鍵生成装置で各カテゴリ用の暗号化メディア鍵データ及び暗号化コンテンツ鍵を生成して記録媒体に記録し、記録装置で暗号化メディア鍵データ及び暗号化コンテンツ鍵を復号してコンテンツを暗号化する構成とすることにより、書き換え型もしくは追記型の記録媒体を用いるシステムにも適用することができる。

【０１７０】

（実施の形態６）

本発明の実施の形態６は、実施の形態１と同様、再生専用の記録媒体を用いてコンテンツを配布し、再生装置でコンテンツを再生するシステムに本発明を適用したものである。

【０１７１】

以下、本発明の実施の形態６について、図面を参照にしながら説明する。図３１は、コンテンツを暗号化して記録する記録装置３１００及び記録媒体３１２０を示しており、図３２は、記録媒体３１２０から暗号化コンテンツを読み出して復号する第１の再生装置３２００を示しており、図３３は、記録媒体３１２０から暗号化コンテンツを読み出して復号する第２の再生装置３３００を示している。また、図３４は記録媒体３１２０に記録される各種データの具体例を示している。

【０１７２】

図３１の記録装置３１００が図１の記録装置１００と異なる点は、コンテンツ鍵生成部３１０９で外部から入力される第１及び第２のシードを用いてコンテンツ鍵を生成し、メディア鍵を用いて第１及び第２のシードをそれぞれ第１のシード暗号化部３１０７及び第２のシード暗号化部３１０８で暗号化して、記録媒体３１２０に記録するようにしたことである。その他の点は図１の記録装置１００と同じであるので、その説明は省略する。

【０１７３】

記録媒体３１２０は、第１の暗号化メディア鍵データを記録する第１の暗号化メディア鍵データ記録領域３１２１と、第２の暗号化メディア鍵データを記録する第２の暗号化メディア鍵データ記録領域３１２２と、第１のシード暗号化部３１０７が生成した第１の暗号化シードを記録する第１の暗号化シード記録領域３１２３と、第２のシード暗号化部３

１０８が生成した第２の暗号化シードを記録する第２の暗号化シード記録領域３１２４と、暗号化コンテンツを記録する暗号化コンテンツ記録領域３１２５とを備える。

【０１７４】

第１の再生装置３２００は、読み出し装置３２１０及び復号装置３２２０とから構成される。

【０１７５】

読み出し装置３２１０は、デバイス鍵を秘密に保有するデバイス鍵格納部３２１１と、デバイス鍵を用いて記録媒体３１２０から読み出した第２の暗号化メディア鍵データを復号してメディア鍵を取得する第２のメディア鍵復号部３２１２と、取得したメディア鍵を用いて記録媒体から読み出した第２の暗号化シードを復号して第２のシードを取得する第２のシード復号部３２１３と、取得した第２のシードを、記録媒体３２２０から読み出した第１の暗号化メディア鍵データ、第１の暗号化シード、及び暗号化コンテンツとともに復号装置３２２０に供給する。本実施の形態において、読み出し装置３２１０は上記した構成要素がハードウェアで実装されており、第２のカテゴリに属するものとした。

【０１７６】

復号装置３２２０は、デバイス鍵を秘密に保有するデバイス鍵格納部３２２１と、デバイス鍵を用いて読み出し装置３２１０から供給される第１の暗号化メディア鍵データを復号してメディア鍵を取得する第１のメディア鍵復号部３２２２と、取得したメディア鍵を用いて読み出し装置３２１０から供給される第１の暗号化シードを復号して第１のシードを取得する第１のシード復号部３２２３と、取得した第１のシードと読み出し装置３２１０から供給される第２のシードを用いてコンテンツ鍵を生成するコンテンツ鍵生成部３２２４と、生成したコンテンツ鍵を用いて読み取り装置３２１０から供給される暗号化コンテンツを復号するコンテンツ復号部３２２５とを備える。本実施の形態において、復号装置３２２０は上記した構成要素がソフトウェアで実装されており、第１のカテゴリに属するものとした。

【０１７７】

第２の再生装置３３００は、第２のカテゴリの再生装置であり、デバイス鍵を秘密に保有するデバイス鍵格納部３３０１と、デバイス鍵を用いて記録媒体３１２０から読み出した第２の暗号化メディア鍵データを復号してメディア鍵を取得するメディア鍵復号部３３０２と、取得したメディア鍵を用いて記録媒体から読み出した第１の暗号化シードを復号して第１のシードを取得する第１のシード復号部３３０３と、取得したメディア鍵を用いて記録媒体３１２０から読み出した第２の暗号化シードを復号して第２のシードを取得する第２のシード復号部３３０４と、取得した第１のシードと第２のシードからコンテンツ鍵を生成するコンテンツ鍵生成部３３０５と、生成したコンテンツ鍵を用いて記録媒体３１２０から読み出した暗号化コンテンツを復号するコンテンツ復号部３３０６とを備える。本実施の形態において、第２の再生装置３３００は上記した構成要素がハードウェアで実装されており、第２のカテゴリに属するものとした。

【０１７８】

本実施の形態ではパソコン上のアプリケーションプログラムのようにソフトウェアで実装される復号装置を第１のカテゴリに属する復号装置とし、一般的な民生プレーヤ及びパソコンに接続もしくは内蔵される光ディスクドライブのようにハードウェアで実装される装置を第２のカテゴリに属する装置とした。

【０１７９】

図３４は、ｍ台の第１のカテゴリの復号装置及びｎ台の第２のカテゴリの装置がそれぞれ固有のデバイス鍵を１個だけ保有しており、第１のカテゴリの復号装置２と第２のカテゴリの装置３が無効化されているとした場合の、記録媒体３１２０に記録される各種データの具体例を示している。図３４中で、第１のカテゴリの復号装置ｉ（ｉ＝１～ｍ）が保有するデバイス鍵をＤＫＡｉ、第２のカテゴリの装置ｊ（ｊ＝１～ｎ）が保有するデバイス鍵をＤＫＡｊとしている。また、Ｅａ（Ｘ，Ｙ）、Ｅｂ（Ｘ，Ｙ）、Ｅｃ（Ｘ，Ｙ）、Ｅｄ（Ｘ，Ｙ）、及びＥｅ（Ｘ，Ｙ）はデータＹを鍵データＸを用いて暗号化する関数を

意味する。なお、使用される暗号アルゴリズムは公知の技術で実現可能であり、本実施の形態では鍵長５６ビットのＤＥＳ暗号を使用した。

【０１８０】

第１の暗号化メディア鍵データ記録領域３１２１及び第２の暗号化メディア鍵データ記録領域３１２２に記録されるデータは、それぞれ、前記した実施の形態１における第１の暗号化メディア鍵データ記録領域１２１及び第２の暗号化メディア鍵データ記録領域１２２に記録されるデータと同じであるので、その説明は省略する。

【０１８１】

（第１の暗号化シード記録領域３１２３）

第１の暗号化シード記録領域３１２３にはメディア鍵（ＭＫ）で暗号化された第１のシード（ＳＤ１）が記録されている。

【０１８２】

（第２の暗号化シード記録領域３１２４）

第２の暗号化シード記録領域３１２４にはメディア鍵（ＭＫ）で暗号化された第２のシード（ＳＤ２）が記録されている。

【０１８３】

（暗号化コンテンツ記録領域３１２５）

暗号化コンテンツ記録領域３１２５には、コンテンツ鍵（ＣＫ）で暗号化されたコンテンツが記録されている。

【０１８４】

以上のように構成された本発明の実施の形態において、例えば第１のカテゴリの復号装置に付与したデバイス鍵の多数や、第１の暗号化メディア鍵データを復号するアルゴリズムがインターネット上で不正に公開され、第１のカテゴリの復号装置の無効化が機能しなくなったと判断された場合には、第１のカテゴリの復号装置の無効化システムを更新することになる。以下、その具体例を説明する。

【０１８５】

（システム更新の具体例１）

第１のカテゴリの復号装置の無効化が機能しなくなったと判断されて以降、新たに作成する記録媒体３１２０に記録する各種データの具体例１を図３５に示す。図３４との違いは、第１の暗号化メディア鍵データの生成に用いるデバイス鍵をＤＫＡ１～ＤＫＡｍからＤＫＡ’１～ＤＫＡ’ｍに変更したことである。これは、前記した実施の形態１で述べたシステム更新の具体例１と同様であるので、詳細についての説明は省略する。

【０１８６】

ここで、新たなデバイス鍵（ＤＫＡ’１～ＤＫＡ’ｍ）のうちの各デバイス鍵は、システム更新前のデバイス鍵（ＤＫＡ１～ＤＫＡｍ）のどれとも一致しないようになっているので、システム更新前に不正な解析行為により暴露されたデバイス鍵がＤＫＡ２以外に存在したとしても、そのデバイス鍵を使って図３５の記録媒体から読み出した第１の暗号化メディア鍵データを復号してメディア鍵（ＭＫ）を取得することはできず、コンテンツを再生することはできない。

【０１８７】

なお、上記したシステム更新に際して、第２の暗号化メディア鍵データの生成に用いるデバイス鍵（ＤＫＢ１～ＤＫＢｎ）は変更されていないので、第２のカテゴリに属する装置には何らの変更を加える必要がない。

【０１８８】

（システム更新の具体例２）

第１のカテゴリの復号装置の無効化が機能しなくなったと判断されて以降、新たに作成する記録媒体３１２０に記録する各種データの具体例２を図３６に示す。図３４との違いは、第１の暗号化メディア鍵データの生成に用いるデバイス鍵をＤＫＡ１～ＤＫＡｍからＤＫＡ’１～ＤＫＡ’ｍに変更したことと、暗号化アルゴリズムをＥａ（Ｘ，Ｙ）からＥａ’（Ｘ，Ｙ）に変更したことである。これは、前記した実施の形態１で述べたシステム

更新の具体例２と同様であるので、詳細についての説明は省略する。

【０１８９】

ここで、新たなデバイス鍵（ＤＫＡ’１～ＤＫＡ’ｍ）のうちの各デバイス鍵は、システム更新前のデバイス鍵（ＤＫＡ１～ＤＫＡｍ）のどれとも一致しないようになっているので、システム更新前に不正な解析行為により暴露されたデバイス鍵がＤＫＡ２以外に存在したとしても、そのデバイス鍵を使って図３６の記録媒体から読み出した第１の暗号化メディア鍵データを復号してメディア鍵（ＭＫ）を取得することはできず、コンテンツを再生することはできない。

【０１９０】

また、デバイス鍵の鍵長や暗号アルゴリズムを変更して暗号強度の高いものにすることができるので、システムを解析してデバイス鍵を不正取得するといった行為を困難にすることができる。

【０１９１】

なお、上記したシステム更新に際して、第２の暗号化メディア鍵データの生成に用いるデバイス鍵（ＤＫＢ１～ＤＫＢｎ）及び第２の暗号化メディア鍵データの暗号化アルゴリズムは変更されていないので、第２のカテゴリに属する装置には何らの変更を加える必要がない。

【０１９２】

以上のように構成された本発明の実施の形態５によれば、第１のカテゴリの装置（復号装置３２２０）及び第２のカテゴリの装置（読み出し装置３２１０及び第２の再生装置３３００）は、それぞれ異なるカテゴリの装置を無効化するための第１もしくは第２の暗号化メディア鍵データを読み込む必要がないため、装置内に設けるメモリ容量を小さくでき、処理時間も短くできる。また、第１の暗号化メディア鍵データの生成に用いる暗号化アルゴリズムを第２の暗号化メディア鍵データの生成に用いる暗号化アルゴリズムと異なるものとすることができるため、第１のカテゴリの復号装置の無効化システムが暴露されるような事態に陥った場合にも、第１のカテゴリの復号装置に付与するデバイス鍵の鍵長や第１の暗号化メディア鍵データの生成アルゴリズムを変更することで、第２のカテゴリの装置に影響を与えることなく、無効化システムを変更することが可能になる。さらに、第１のカテゴリの復号装置３２２０には、第２の暗号化シードを復号するためのアルゴリズムは実装されていないので、第１のカテゴリの復号装置の何れかを解析して保有するデバイス鍵や復号アルゴリズムを暴露したとしても、コンテンツ毎に異なる第２の暗号化シードを復号することはできず、第１のカテゴリに対する不正行為がシステム全体に影響することを防ぐことができ、より堅牢な著作権保護システムを構築できる。これは、本実施の形態のように第１のカテゴリは復号アルゴリズムや鍵の更新や追加が容易ではあるが堅牢な実装が困難なソフトウェアで実装される復号装置とし、第２のカテゴリは堅牢ではあるが復号アルゴリズムや鍵の更新や追加が困難なハードウェアで実装される再生装置もしくは読み取り装置とした場合に、特に有効である。

【０１９３】

なお、図３１で、メディア鍵、第１のシード、及び第２のシードが記録装置３１００の外部から入力される形態としたが、本発明はその構成に限定されるものではない。例えば、記録装置３１００がメディア鍵、第１のシード、及び第２のシードを格納する格納部を有する構成であってもよい。また、記録装置３１００がメディア鍵、第１のシード、及び第２のシードをその都度生成する生成部を有する構成であってもよい。

【０１９４】

また、図３１では、第１のシード及び第２のシードからコンテンツ鍵を生成し、コンテンツをコンテンツ鍵で暗号化し、第１及び第２のシードをメディア鍵で暗号化する構成としたが、本発明はそれに限定されるものではない。例えば、鍵を追加して暗号化の階層をさらに増やす構成であってもよい。

【０１９５】

また、本実施の形態では記録装置として図３１に示すように、各カテゴリのデバイス鍵

格納部、メディア鍵暗号化部、シード暗号化部、コンテンツ鍵生成部、コンテンツ暗号化部及び記録媒体への各データの記録が一体の構成としたが、本発明はそれに限定されるものではなく、記録装置が分離して構成されるものであっても良い。例えば、各カテゴリのデバイス鍵格納部、メディア鍵暗号化部、シード暗号化部、及びコンテンツ鍵生成部（図３１中の破線で囲んだ部分）は、その管理、運用に高い秘匿性が要求されることから、システム全体の鍵管理や再生装置に対する鍵発行等を運用する機関に設置される装置に内蔵され、コンテンツ暗号部や記録媒体に各データへの記録はコンテンツ製造機関や記録媒体製造機関に設置される装置で実行される形態であっても良い。

【０１９６】

また、本実施の形態ではシステム更新において第１の暗号化メディア鍵データを生成する際に、図３５のＥａ（ＤＫＡ’２，０）や図３６のＥａ’（ＤＫＡ’２，０）のようにシステム更新の時点で無効化されている復号装置にもデータを割り当てる構成としているが、無効化されている復号装置にはデータを割り当てない構成とすることも可能である。その場合、無効化されていない復号装置の使うべき暗号化メディア鍵の位置も更新し、新たなデバイス鍵を付与する際に新たな位置情報も付与することで、システム更新の前後において暗号化メディア鍵の位置が変わったとしても無効化されていない復号装置は適切なデータを用いることができ、正しいメディア鍵を得ることができる。こうした場合、システム更新後の第１の暗号化メディア鍵データ記録領域に格納すべきデータの容量を削減することができる。あるいは容量の最大値が限定されている場合は新たに第１のカテゴリに属する復号装置の台数を増やすことが可能となる。

【０１９７】

また、本実施の形態では、図３４に示すような暗号化メディア鍵データを用いて復号装置の無効化を行う方法としたが、無効化の方法は他の方法を利用してもよく、例えば特許文献１として開示されている木構造を利用した無効化方法を用いても良い。

【０１９８】

また、本実施の形態では、暗号アルゴリズムとして鍵長５６ｂｉｔのＤＥＳ、あるいはシステム更新後の暗号アルゴリズムとして鍵長１１２ｂｉｔの２キートリプルＤＥＳを用いたが、本発明はこれに限定されるものではなく、他の暗号アルゴリズム、例えば次世代の標準暗号とされる鍵長１２８ｂｉｔのＡＥＳ等を用いても良い。

【０１９９】

なお、本実施の形態は、再生専用の記録媒体を用いてコンテンツを配布し、再生装置でコンテンツを再生するシステムに本発明を適用したものであるが、本発明はそれに限定されるものではない。前記した実施の形態２のように、鍵生成装置で各カテゴリ用の暗号化メディア鍵データ及び暗号化シードを生成して記録媒体に記録し、記録装置で暗号化メディア鍵データ及び暗号化シードを復号し、コンテンツ鍵を生成し、コンテンツを暗号化する構成とすることにより、書き換え型もしくは追記型の記録媒体を用いるシステムにも適用することができる。

【０２００】

（実施の形態７）

本発明の実施の形態７は、実施の形態６のシステムにおいて、第１のカテゴリと第２のカテゴリに対して個別にメディア鍵を設け、それぞれを用いた第１の暗号化シードの階層を設けるようにしたものである。

【０２０１】

以下、本発明の実施の形態７について、図面を参照にしながら説明する。図３７は、コンテンツを暗号化して記録する記録装置３７００及び記録媒体３７２０を示しており、図３８は、記録媒体３７２０から暗号化コンテンツを読み出して復号する第１の再生装置３８００を示しており、図３９は、記録媒体３７２０から暗号化コンテンツを読み出して復号する第２の再生装置３９００を示している。また、図４０は記録媒体３７２０に記録される各種データの具体例を示している。

【０２０２】

図３７の記録装置３７００が図３１の記録装置３１００と異なる点は、第１のカテゴリに対しては第１のメディア鍵を、第２のカテゴリに対しては第２のメディア鍵を、個別に設け、第１及び第２のメディア鍵をそれぞれ第１のメディア鍵暗号化部３７０５及び第２のメディア鍵暗号化部３７０６で暗号化し、第１のシードを第１及び第２のメディア鍵を用いてそれぞれ第１シード暗号化部（１）３７０７及び第１のシード暗号化部（２）３７１１で暗号化し、記録媒体３７２０に記録するようにしたことである。その他の点については、前記した実施の形態６の記録装置３１００と同じであるので、その説明は省略する。

【０２０３】

記録媒体３７２０は、第１の暗号化メディア鍵データを記録する第１の暗号化メディア鍵データ記録領域３７２１と、第２の暗号化メディア鍵データを記録する第２の暗号化メディア鍵データ記録領域３７２２と、第１のシード暗号化部（１）３７０７が生成した第１の暗号化シード（１）を記録する第１の暗号化シード（１）記録領域３７２３と、第１のシード暗号化部（２）３７１１が生成した第１の暗号化シード（２）を記録する第１の暗号化シード（２）記録領域３７２６と、第２の暗号化シードを記録する第２の暗号化シードデータ記録領域３７２４と、暗号化コンテンツを記録する暗号化コンテンツ記録領域３７２５とを備える。

【０２０４】

第１の再生装置３８００において復号装置３８２０は、読み出し装置３８１０が記録媒体３７２０から読み出した第１の暗号化シード（１）を復号して第１のシードを取得する。その他の点については、前記した実施の形態６における第１の再生装置３２００と同様であるので、その説明は省略する。

【０２０５】

第２の再生装置３９００は、記録媒体３７２０から読み出した第１の暗号化シード（２）を復号して第１のシードを取得する。その他の点については、前記した実施の形態６における第２の再生装置３３００と同様であるので、その説明は省略する。

【０２０６】

図４０は、記録媒体３７２０に記録される各種データの具体例を示している。第１の暗号化メディア鍵データ記録領域３７２１には、第１のカテゴリの復号装置が保有するデバイス鍵（ＤＫＡ１～ＤＫＡｍ）で暗号化された第１のメディア鍵（ＭＫ１）が記録されており、第２の暗号化メディア鍵データ記録領域３７２２には、第２のカテゴリの装置が保有するデバイス鍵（ＤＫＢ１～ＤＫＢｍ）で暗号化された第２のメディア鍵（ＭＫ２）がきろくされている。また、第１の暗号化シードデータ（１）記録領域３７２３には、第１のメディア鍵（ＭＫ１）で暗号化された第１のシード（ＳＤ１）が記録されており、第１の暗号化シードデータ（２）記録領域３７２６には、第２のメディア鍵（ＭＫ２）で暗号化された第１のシード（ＳＤ１）が記録されている。その他の点については、前記した図３４と同じであるので、説明を省略する。なお、図４０中の、Ｅｆ（Ｘ，Ｙ）はデータＹを鍵データＸを用いて暗号化する関数を意味し、本実施の形態では鍵長５６ビットのＤＥＳ暗号を使用した。

【０２０７】

以上のように構成された本発明の実施の形態７において、例えば第１のカテゴリの復号装置に付与したデバイス鍵の多数や、第１の暗号化メディア鍵データを復号するアルゴリズムがインターネット上で不正に公開され、第１のカテゴリの復号装置の無効化が機能しなくなったと判断された場合には、第１のカテゴリの復号装置の無効化システムを更新することになる。以下、その具体例を説明する。

【０２０８】

（システム更新の具体例１）

第１のカテゴリの復号装置の無効化が機能しなくなったと判断されて以降、新たに作成する記録媒体３７２０に記録する各種データの具体例１を図４１に示す。図４０との違いは、第１の暗号化メディア鍵データの生成に用いるデバイス鍵をＤＫＡ１～ＤＫＡｍから

ＤＫＡ’１～ＤＫＡ’ｍに変更したことである。これは、前記した実施の形態１で述べたシステム更新の具体例１と同様であるので、詳細についての説明は省略する。

【０２０９】

（システム更新の具体例２）

第１のカテゴリの復号装置の無効化が機能しなくなったと判断されて以降、新たに作成する記録媒体３７２０に記録する各種データの具体例２を図４２に示す。図４０との違いは、第１の暗号化メディア鍵データの生成に用いるデバイス鍵をＤＫＡ１～ＤＫＡｍからＤＫＡ’１～ＤＫＡ’ｍに変更したこと、暗号化アルゴリズムをＥａ（Ｘ，Ｙ）からＥａ’（Ｘ，Ｙ）に変更したこと、及び第１の暗号化シード（１）の暗号化アルゴリズムをＥｃ（Ｘ，Ｙ）からＥｃ’（Ｘ，Ｙ）に変更したことである。これは、前記した実施の形態３で述べたシステム更新の具体例２と同様であるので、詳細についての説明は省略する。

【０２１０】

以上のように構成された本発明の実施の形態７によれば、前記した実施の形態６同様に、堅牢な著作権保護システムを構築できる。さらに、本実施の形態では第１のカテゴリと第２のカテゴリに対して個別にメディア鍵を設け、それぞれを用いた暗号化シードの階層を設けることにより、カテゴリ間の独立性を高めることが可能となる。すなわち第１のカテゴリに属する装置からデバイス鍵が暴露された場合であっても、それを用いて得られるメディア鍵は第１のメディア鍵のみであり、第２のメディア鍵が暴露されることを防ぐことが可能となる。これは、本実施の形態のように第１のカテゴリは復号アルゴリズムや鍵の更新や追加が容易ではあるが堅牢な実装が困難なソフトウェアで実装される復号装置とし、第２のカテゴリは堅牢ではあるが復号アルゴリズムや鍵の更新や追加が困難なハードウェアで実装される再生装置もしくは読み取り装置とした場合に、特に有効である

なお、図３７で、第１のメディア鍵、第２のメディア鍵、第１のシード、及び第２のシードが記録装置３７００の外部から入力される形態としたが、本発明はその構成に限定されるものではない。例えば、記録装置３７００がこれらを格納する格納部を有する構成であってもよい。また、記録装置３７００がこれらをその都度生成する生成部を有する構成であってもよい。

【０２１１】

また、図３７では、第１のシード及び第２のシードからコンテンツ鍵を生成し、コンテンツをコンテンツ鍵で暗号化し、第１及び第２のシードをメディア鍵で暗号化する構成としたが、本発明はそれに限定されるものではない。例えば、鍵を追加して暗号化の階層をさらに増やす構成であってもよい。

【０２１２】

また、本実施の形態では記録装置として図３７に示すように、各カテゴリのデバイス鍵格納部、メディア鍵暗号化部、シード暗号化部、コンテンツ鍵生成部、コンテンツ暗号化部及び記録媒体への各データの記録が一体の構成としたが、本発明はそれに限定されるものではなく、記録装置が分離して構成されるものであっても良い。例えば、各カテゴリのデバイス鍵格納部、メディア鍵暗号化部、シード暗号化部、及びコンテンツ鍵生成部（図３７中の破線で囲んだ部分）は、その管理、運用に高い秘匿性が要求されることから、システム全体の鍵管理や再生装置に対する鍵発行等を運用する機関に設置される装置に内蔵され、コンテンツ暗号部や記録媒体に各データへの記録はコンテンツ製造機関や記録媒体製造機関に設置される装置で実行される形態であっても良い。

【０２１３】

また、本実施の形態ではシステム更新において第１の暗号化メディア鍵データを生成する際に、図４１のＥａ（ＤＫＡ’２，０）や図４２のＥａ’（ＤＫＡ’２，０）のようにシステム更新の時点で無効化されている復号装置にもデータを割り当てる構成としているが、無効化されている復号装置にはデータを割り当てない構成とすることも可能である。その場合、無効化されていない復号装置の使うべき暗号化メディア鍵の位置も更新し、新たなデバイス鍵を付与する際に新たな位置情報も付与することで、システム更新の前後において暗号化メディア鍵の位置が変わったとしても無効化されていない復号装置は適切な

データを用いることができ、正しいメディア鍵を得ることができる。こうした場合、システム更新後の第１の暗号化メディア鍵データ記録領域に格納すべきデータの容量を削減することができる。あるいは容量の最大値が限定されている場合は新たに第１のカテゴリに属する復号装置の台数を増やすことが可能となる。

【０２１４】

また、本実施の形態では、図４０に示すような暗号化メディア鍵データを用いて復号装置の無効化を行う方法としたが、無効化の方法は他の方法を利用してもよく、例えば特許文献１として開示されている木構造を利用した無効化方法を用いても良い。

【０２１５】

また、本実施の形態では、暗号アルゴリズムとして鍵長５６ｂｉｔのＤＥＳ、あるいはシステム更新後の暗号アルゴリズムとして鍵長１１２ｂｉｔの２キートリプルＤＥＳを用いたが、本発明はこれに限定されるものではなく、他の暗号アルゴリズム、例えば次世代の標準暗号とされる鍵長１２８ｂｉｔのＡＥＳ等を用いても良い。

【０２１６】

なお、本実施の形態は、再生専用の記録媒体を用いてコンテンツを配布し、再生装置でコンテンツを再生するシステムに本発明を適用したものであるが、本発明はそれに限定されるものではない。前記した実施の形態２のように、鍵生成装置で各カテゴリ用の暗号化メディア鍵データ及び暗号化シードを生成して記録媒体に記録し、記録装置で暗号化メディア鍵データ及び暗号化シードを復号し、コンテンツ鍵を生成し、コンテンツを暗号化する構成とすることにより、書き換え型もしくは追記型の記録媒体を用いるシステムにも適用することができる。

【産業上の利用可能性】

【０２１７】

本発明にかかる著作権保護システムは、装置内に設けるメモリのサイズを小さくでき、かつ、あるカテゴリの装置が不正に解析されてアルゴリズムや多数の鍵が暴露された場合にも、そのカテゴリの装置用の暗号化・復号のアルゴリズムや鍵長を変更することで、他のカテゴリの装置に何らの変更を加えることなく、システム全体の無効化機能を維持できるという効果があり、著作物をデジタル化したコンテンツを光ディスク等の大容量記録媒体に記録もしくは再生するシステムにおいて、復号アルゴリズムや鍵の更新や追加が容易ではあるが堅牢な実装が困難なソフトウェアで実装される記録装置もしくは再生装置と、堅牢ではあるが復号アルゴリズムや鍵の更新や追加が困難なハードウェアで実装される記録装置もしくは再生装置とが存在するような場合に有用である。

【図面の簡単な説明】

【０２１８】

【図１】本発明の実施の形態１における記録装置及び記録媒体を示すブロック図

【図２】本発明の実施の形態１における記録媒体及び第１のカテゴリの再生装置を示すブロック図

【図３】本発明の実施の形態１における記録媒体及び第２のカテゴリの再生装置を示すブロック図

【図４】本発明の実施の形態１における記録媒体に記録するデータの具体例を示す模式図

【図５】本発明の実施の形態１におけるシステム更新の具体例１を示す模式図

【図６】本発明の実施の形態１におけるシステム更新の具体例２を示す模式図

【図７】本発明の実施の形態２における鍵生成装置及び記録媒体を示すブロック図

【図８】本発明の実施の形態２における第１のカテゴリの記録装置及び記録媒体を示すブロック図

【図９】本発明の実施の形態２における第２のカテゴリの記録装置及び記録媒体を示すブロック図

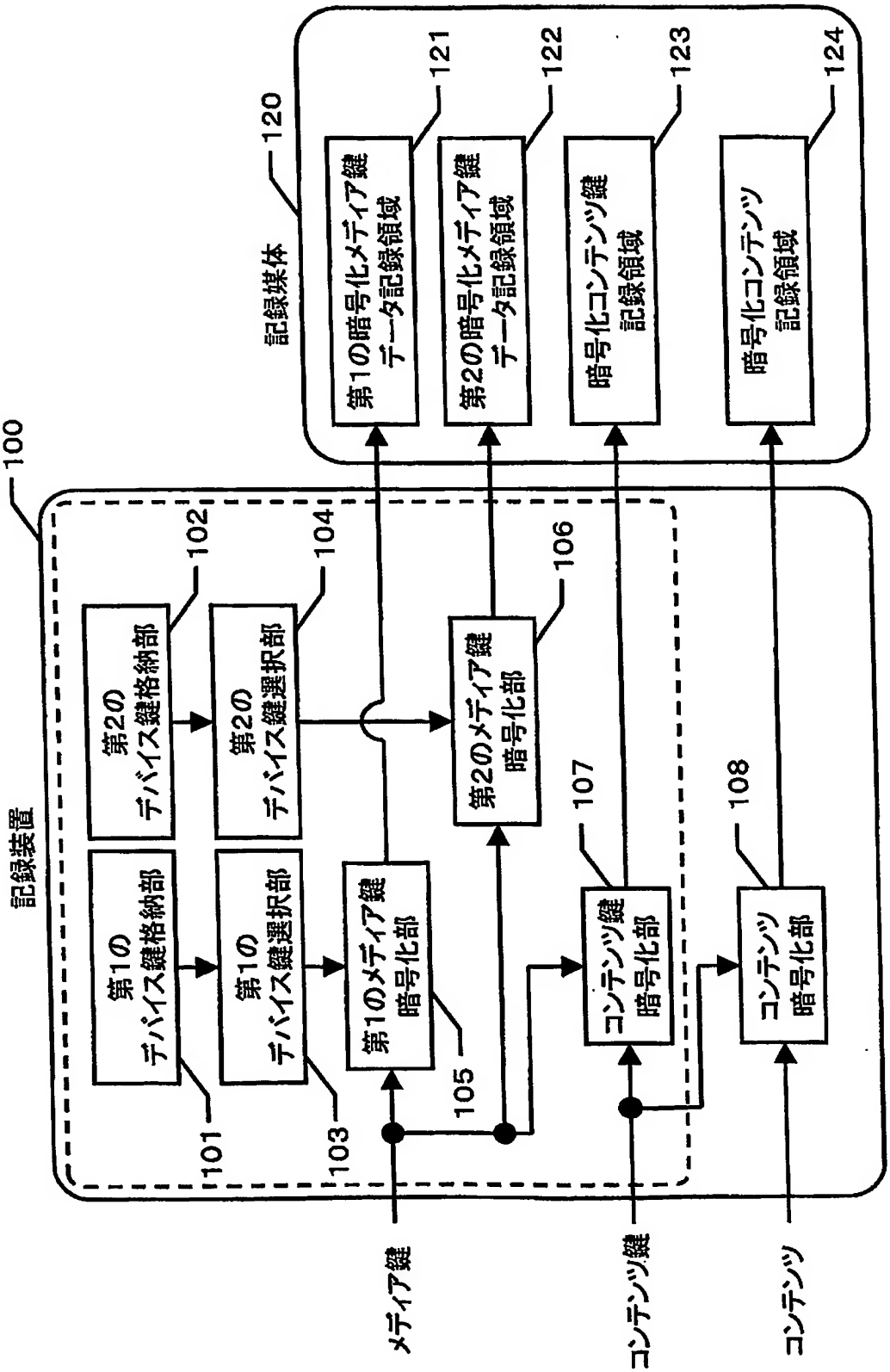
【図１０】本発明の実施の形態２における記録媒体及び第１のカテゴリの再生装置を示すブロック図

【図１１】本発明の実施の形態２における記録媒体及び第２のカテゴリの再生装置を示すブロック図
【図１２】本発明の実施の形態２における記録媒体に記録するデータの具体例を示す模式図
【図１３】本発明の実施の形態３における記録装置及び記録媒体を示すブロック図
【図１４】本発明の実施の形態３における記録媒体及び第１のカテゴリの再生装置を示すブロック図
【図１５】本発明の実施の形態３における記録媒体及び第２の再生装置を示すブロック図
【図１６】本発明の実施の形態３における記録媒体に記録するデータの具体例を示す模式図
【図１７】本発明の実施の形態３におけるシステム更新の具体例１を示す模式図
【図１８】本発明の実施の形態３におけるシステム更新の具体例２を示す模式図
【図１９】本発明の実施の形態４における記録装置及び記録媒体を示すブロック図
【図２０】本発明の実施の形態４における記録媒体及び第１の再生装置を示すブロック図
【図２１】本発明の実施の形態４における記録媒体及び第２の再生装置を示すブロック図
【図２２】本発明の実施の形態４における記録媒体に記録するデータの具体例を示す模式図
【図２３】本発明の実施の形態４におけるシステム更新の具体例１を示す模式図
【図２４】本発明の実施の形態４におけるシステム更新の具体例２を示す模式図
【図２５】本発明の実施の形態５における記録装置及び記録媒体を示すブロック図
【図２６】本発明の実施の形態５における記録媒体及び第１の再生装置を示すブロック図
【図２７】本発明の実施の形態５における記録媒体及び第２の再生装置を示すブロック図
【図２８】本発明の実施の形態５における記録媒体に記録するデータの具体例を示す模式図
【図２９】本発明の実施の形態５におけるシステム更新の具体例１を示す模式図
【図３０】本発明の実施の形態５におけるシステム更新の具体例２を示す模式図
【図３１】本発明の実施の形態６における記録装置及び記録媒体を示すブロック図
【図３２】本発明の実施の形態６における記録媒体及び第１の再生装置を示すブロック図
【図３３】本発明の実施の形態６における記録媒体及び第２の再生装置を示すブロック図
【図３４】本発明の実施の形態６における記録媒体に記録するデータの具体例を示す模式図
【図３５】本発明の実施の形態６におけるシステム更新の具体例１を示す模式図
【図３６】本発明の実施の形態６におけるシステム更新の具体例２を示す模式図
【図３７】本発明の実施の形態７における記録装置及び記録媒体を示すブロック図
【図３８】本発明の実施の形態７における記録媒体及び第１の再生装置を示すブロック図
【図３９】本発明の実施の形態７における記録媒体及び第２の再生装置を示すブロック図
【図４０】本発明の実施の形態７における記録媒体に記録するデータの具体例を示す模式図
【図４１】本発明の実施の形態７におけるシステム更新の具体例１を示す模式図
【図４２】本発明の実施の形態７におけるシステム更新の具体例２を示す模式図
【符号の説明】

【０２１９】
１００　記録装置
１０１　第１のデバイス鍵格納部
１０２　第２のデバイス鍵格納部
１０３　第１のデバイス鍵選択部
１０４　第２のデバイス鍵選択部
１０５　第１のメディア鍵暗号化部
１０６　第２のメディア鍵暗号化部
１０７　コンテンツ鍵暗号化部
１０８　コンテンツ暗号化部
１２０　記録媒体
１２１　第１の暗号化メディア鍵データ記録領域
１２２　第２の暗号化メディア鍵データ記録領域
１２３　暗号化コンテンツ鍵データ記録領域
１２４　暗号化コンテンツ記録領域

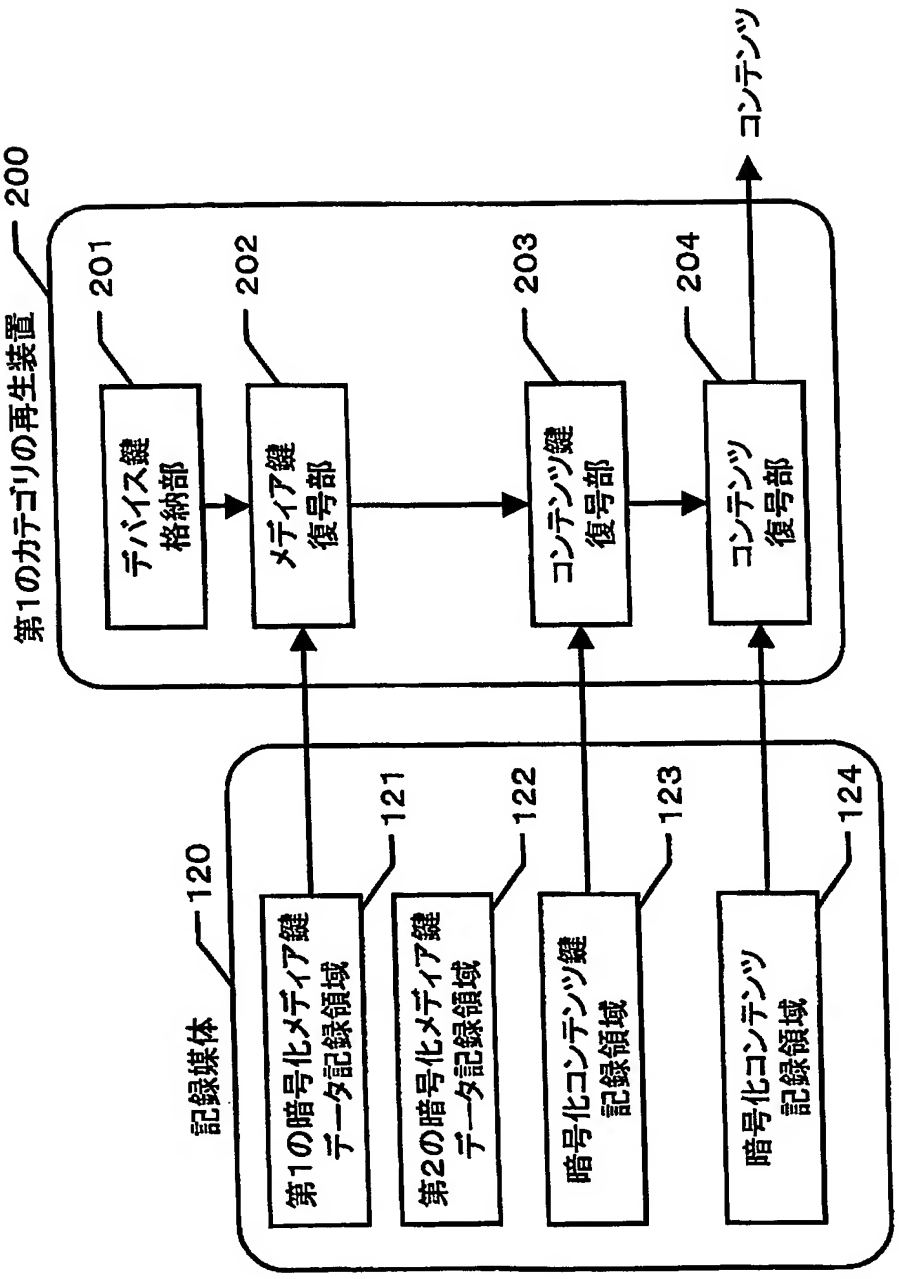
【書類名】図面
【図１】

本発明の実施の形態１における記録装置及び記録媒体



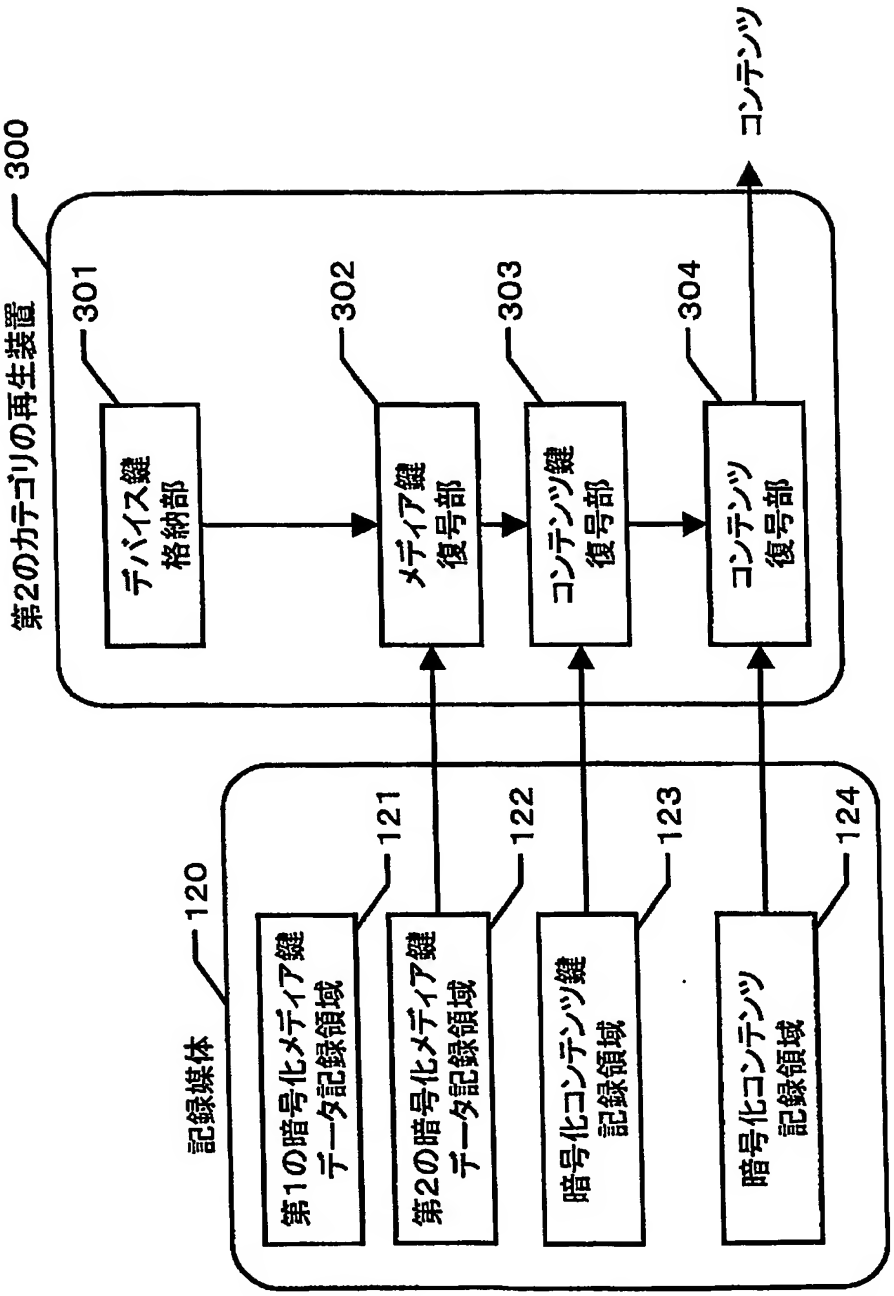
【図２】

本発明の実施の形態１における記録媒体及び第１のカテゴリの再生装置



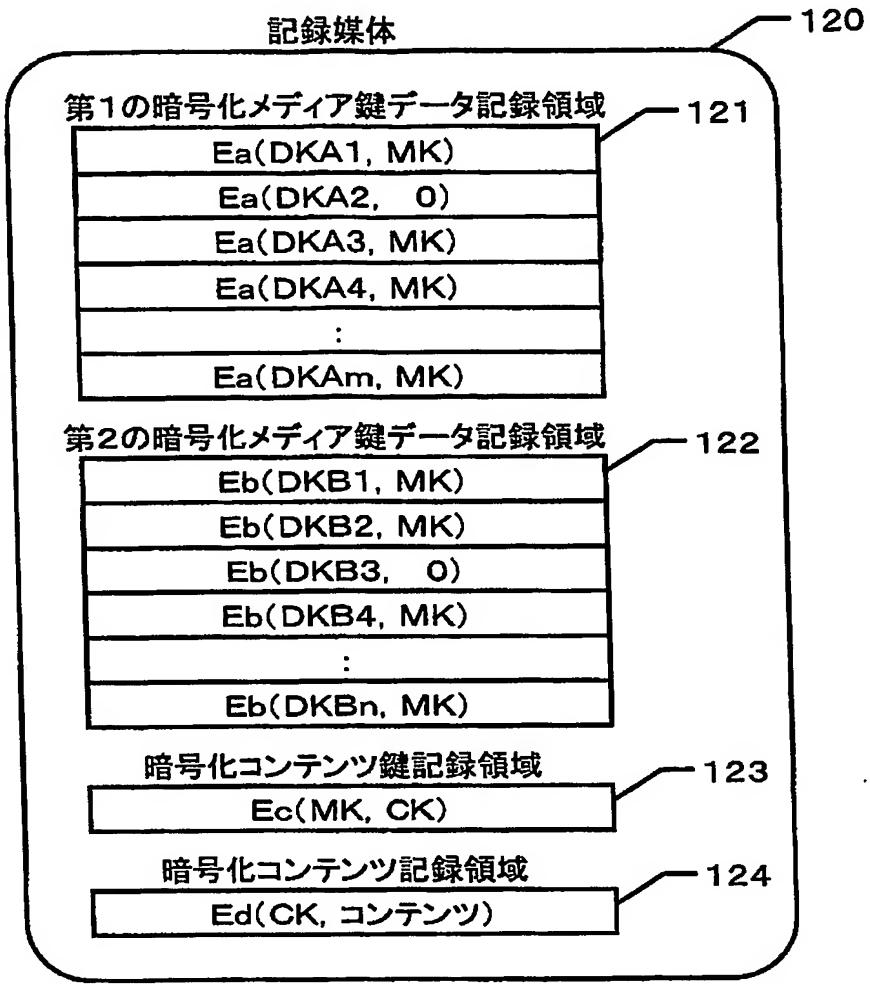
【図３】

本発明の実施の形態１における記録媒体及び第２のカテゴリの再生装置



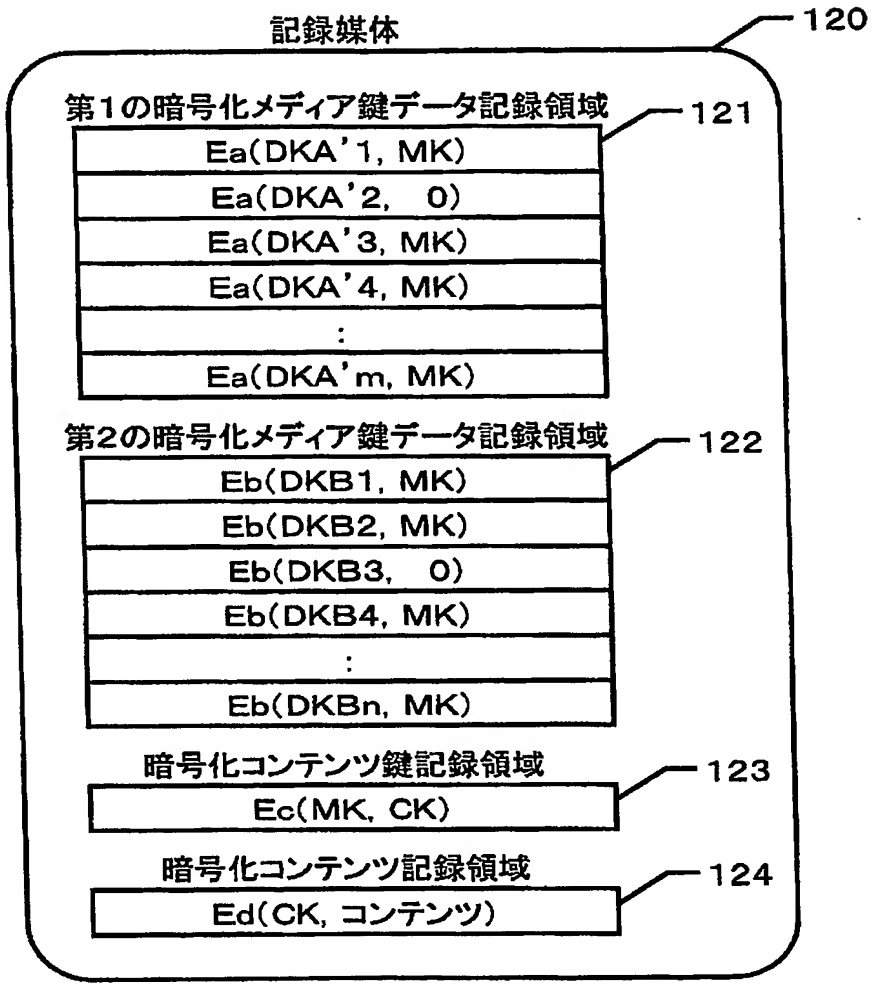
【図４】

本発明の実施の形態1における記録媒体に記録するデータの具体例



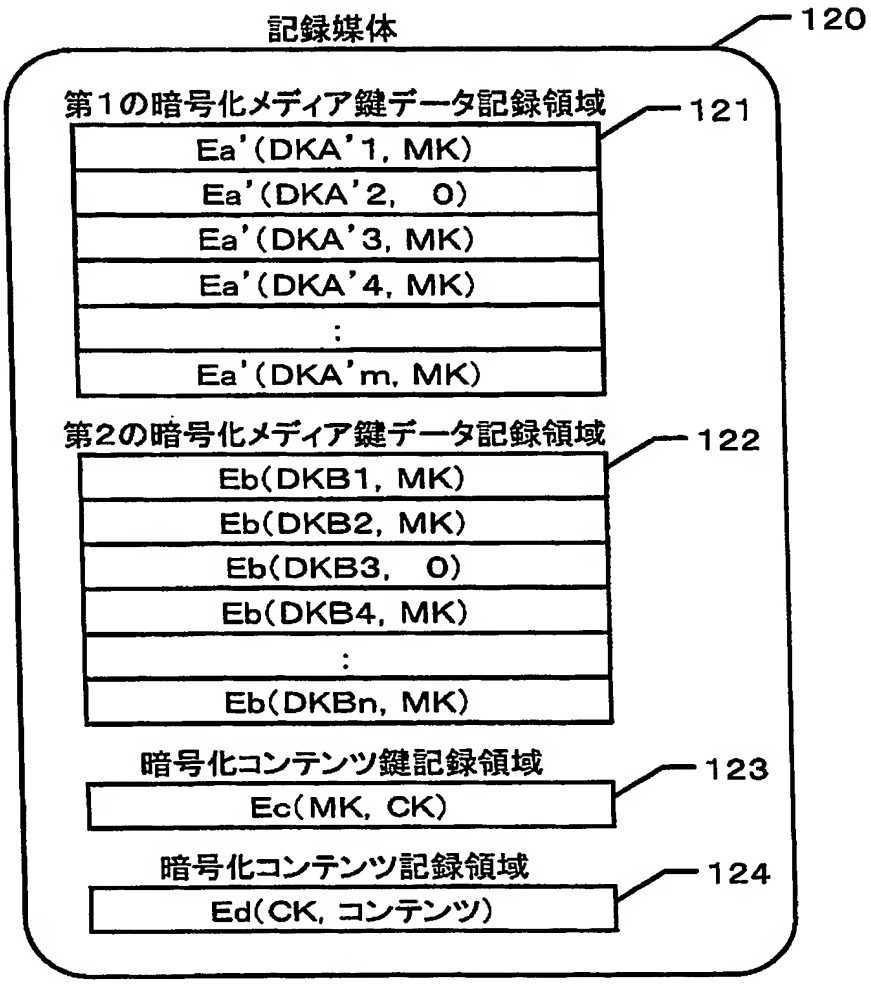
【図５】

本発明の実施の形態１におけるシステム更新の具体例１



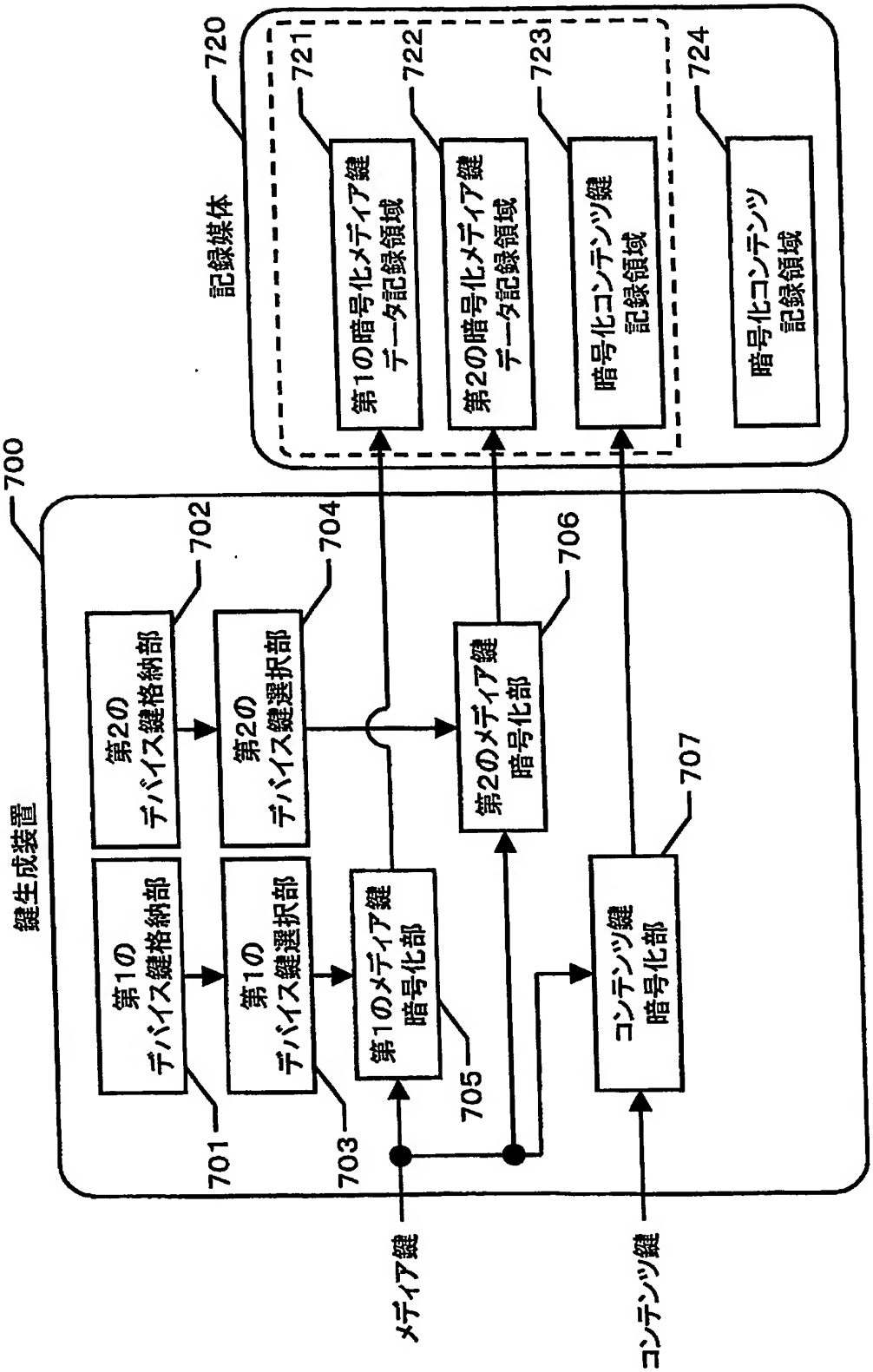
【図６】

本発明の実施の形態1におけるシステム更新の具体例2



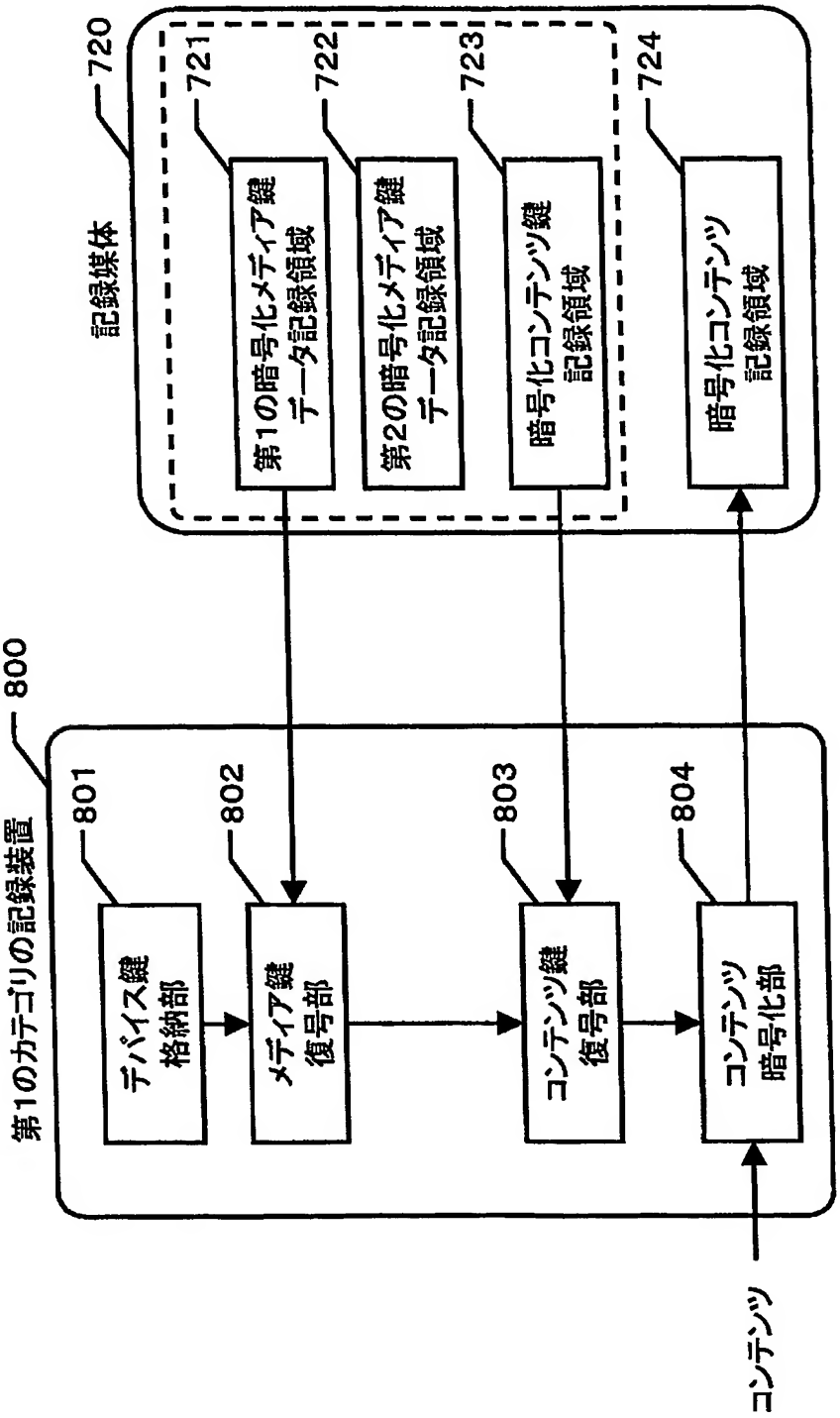
【図７】

本発明の実施の形態2における鍵生成装置及び記録媒体



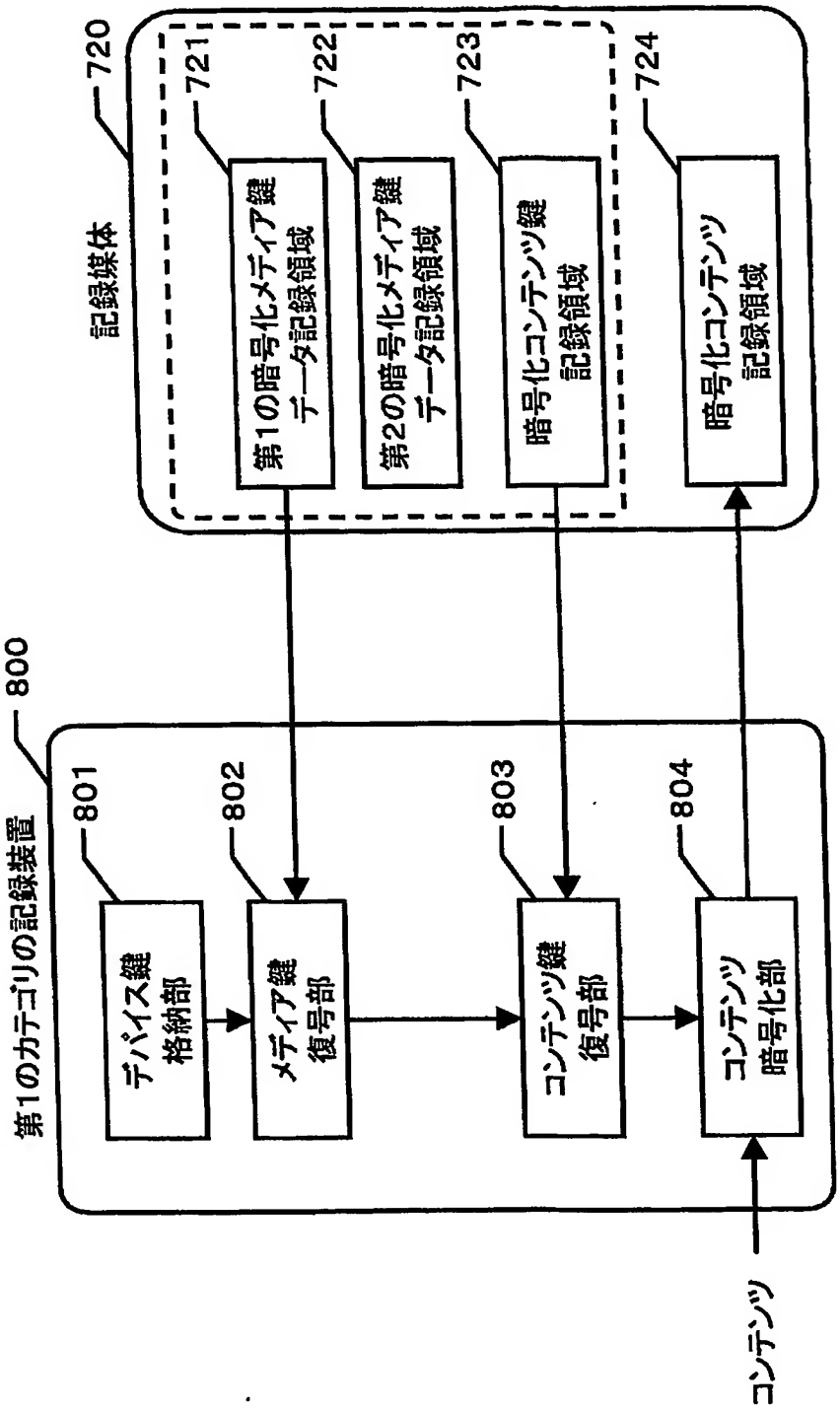
【図８】

本発明の実施の形態2における第1のカテゴリの記録装置及び記録媒体



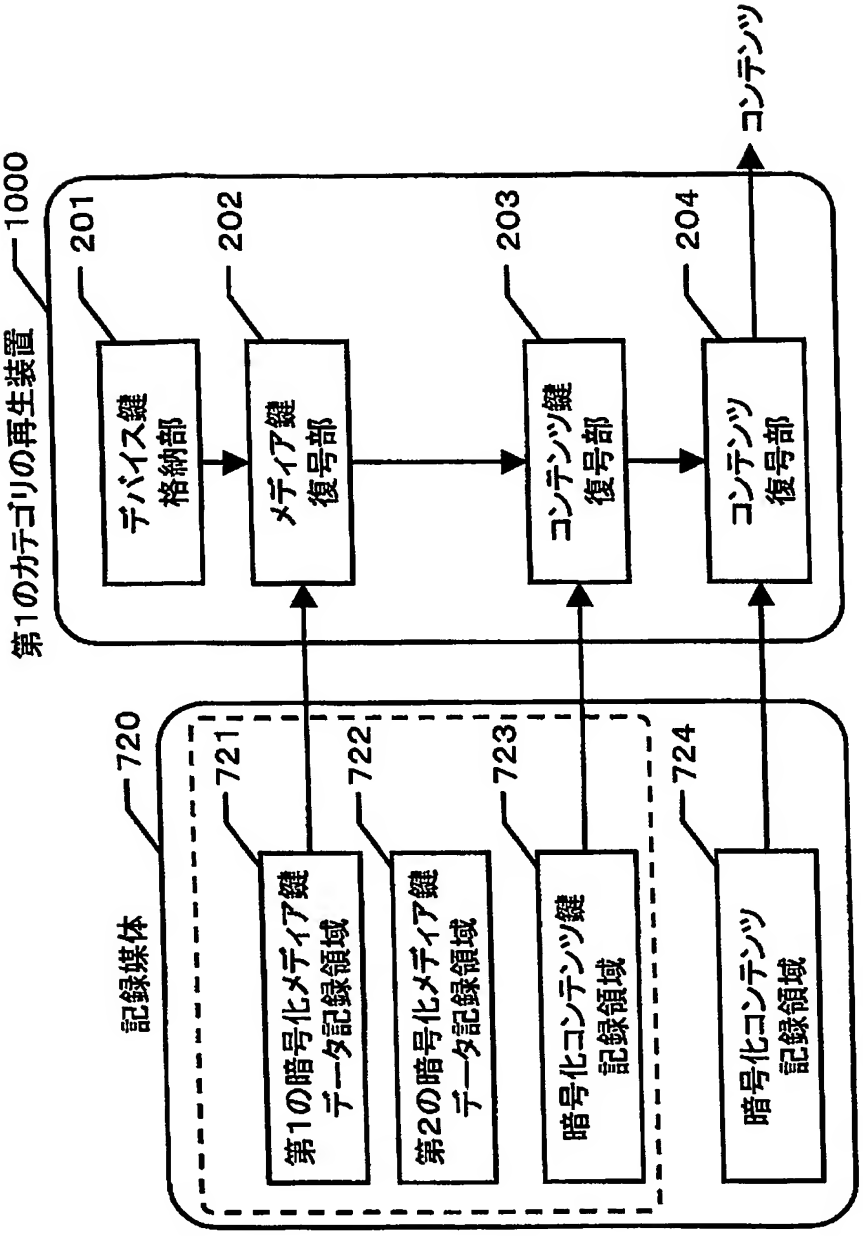
【図９】

本発明の実施の形態2における第1のカテゴリの記録装置及び記録媒体



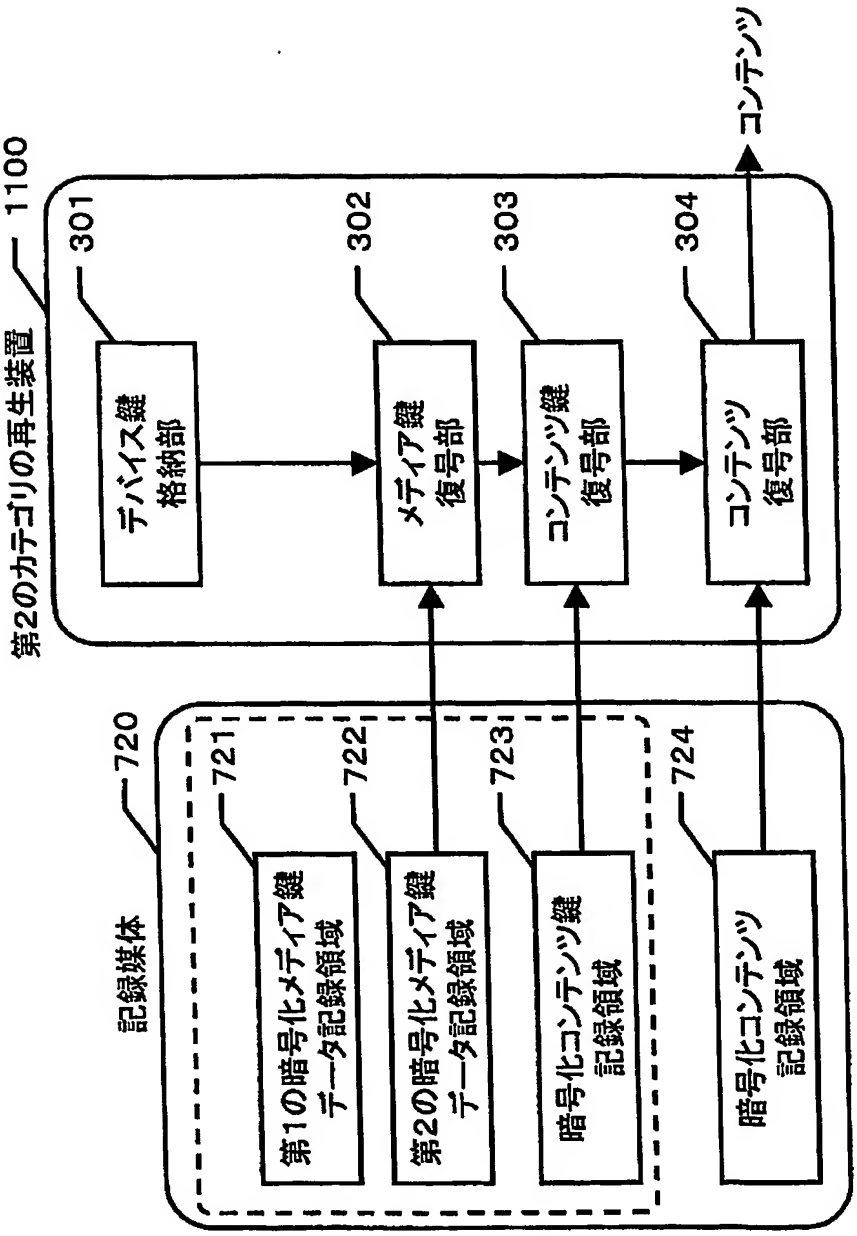
【図１０】

本発明の実施の形態2における記録媒体及び第1のカテゴリの再生装置



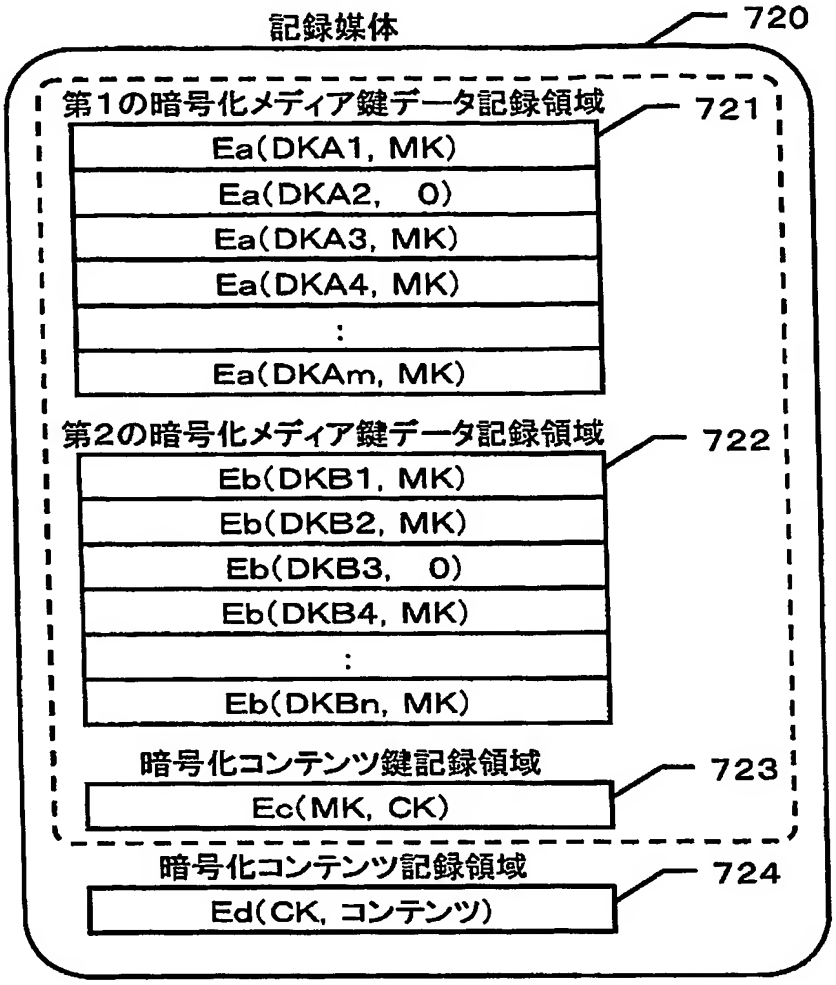
【図１１】

本発明の実施の形態2における記録媒体及び第2のカテゴリの再生装置



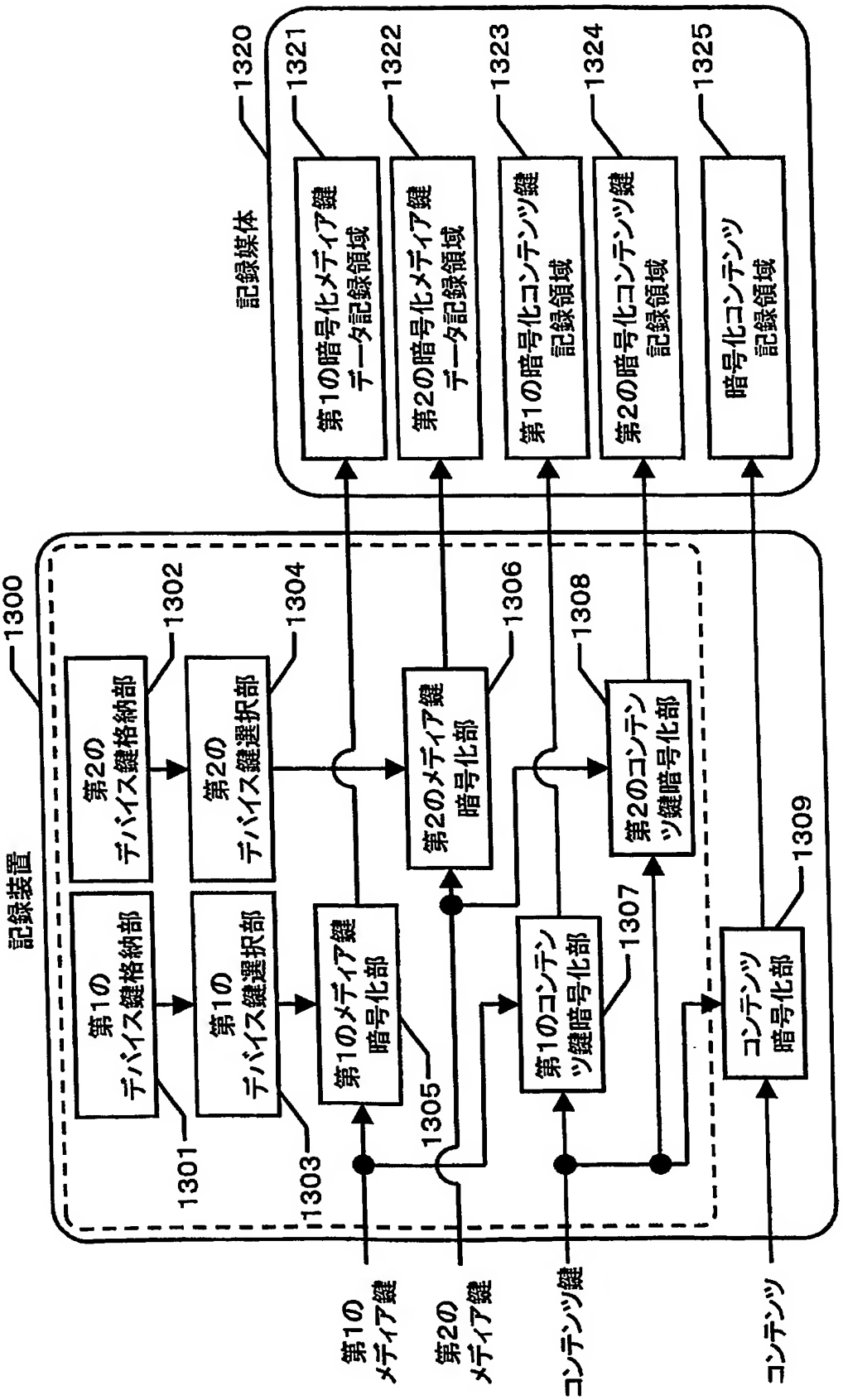
【図１２】

本発明の実施の形態2における記録媒体に記録するデータの具体例



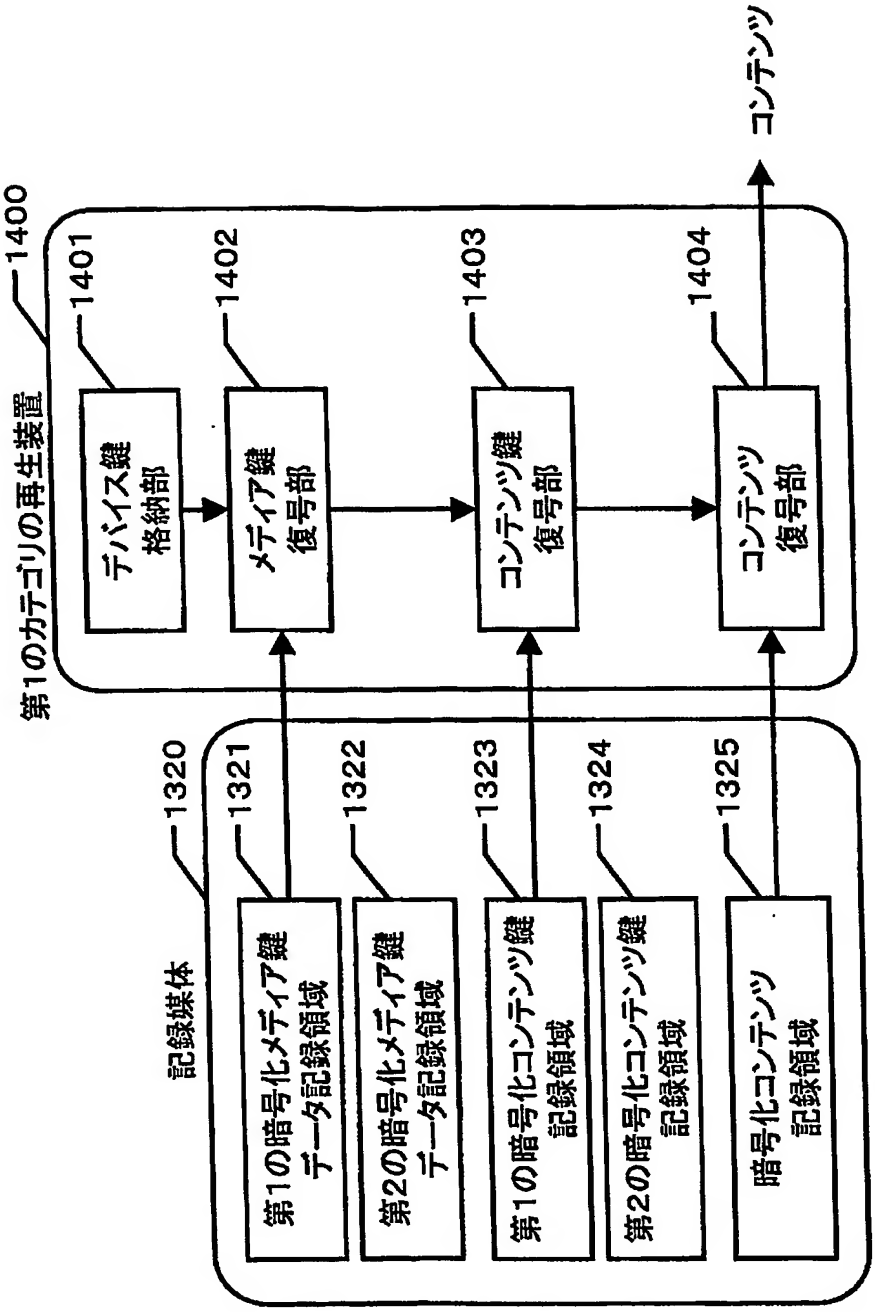
【図１３】

本発明の実施の形態3における記録装置及び記録媒体



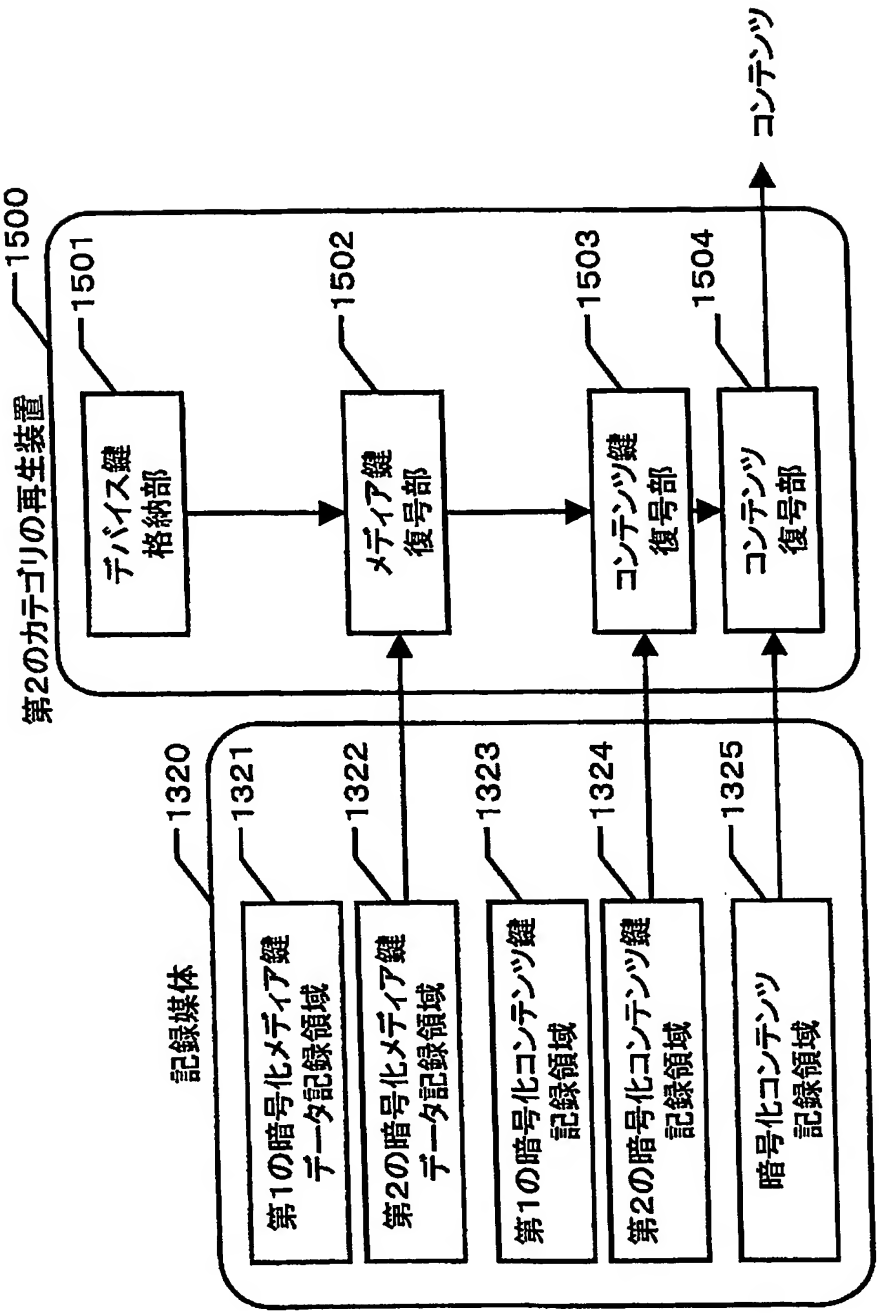
【図１４】

本発明の実施の形態3における記録媒体及び第1のカテゴリの再生装置



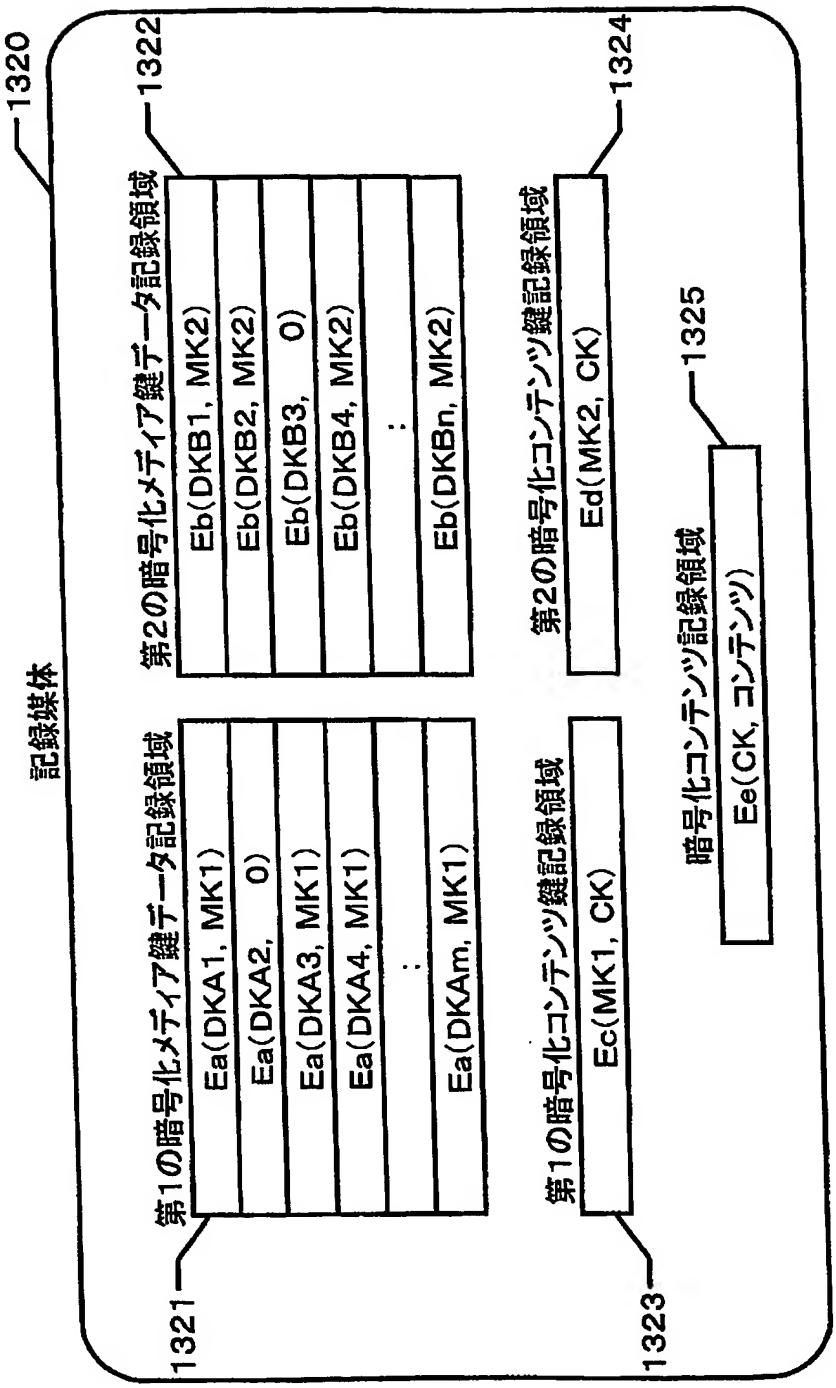
【図１５】

本発明の実施の形態3における記録媒体及び第2の再生装置



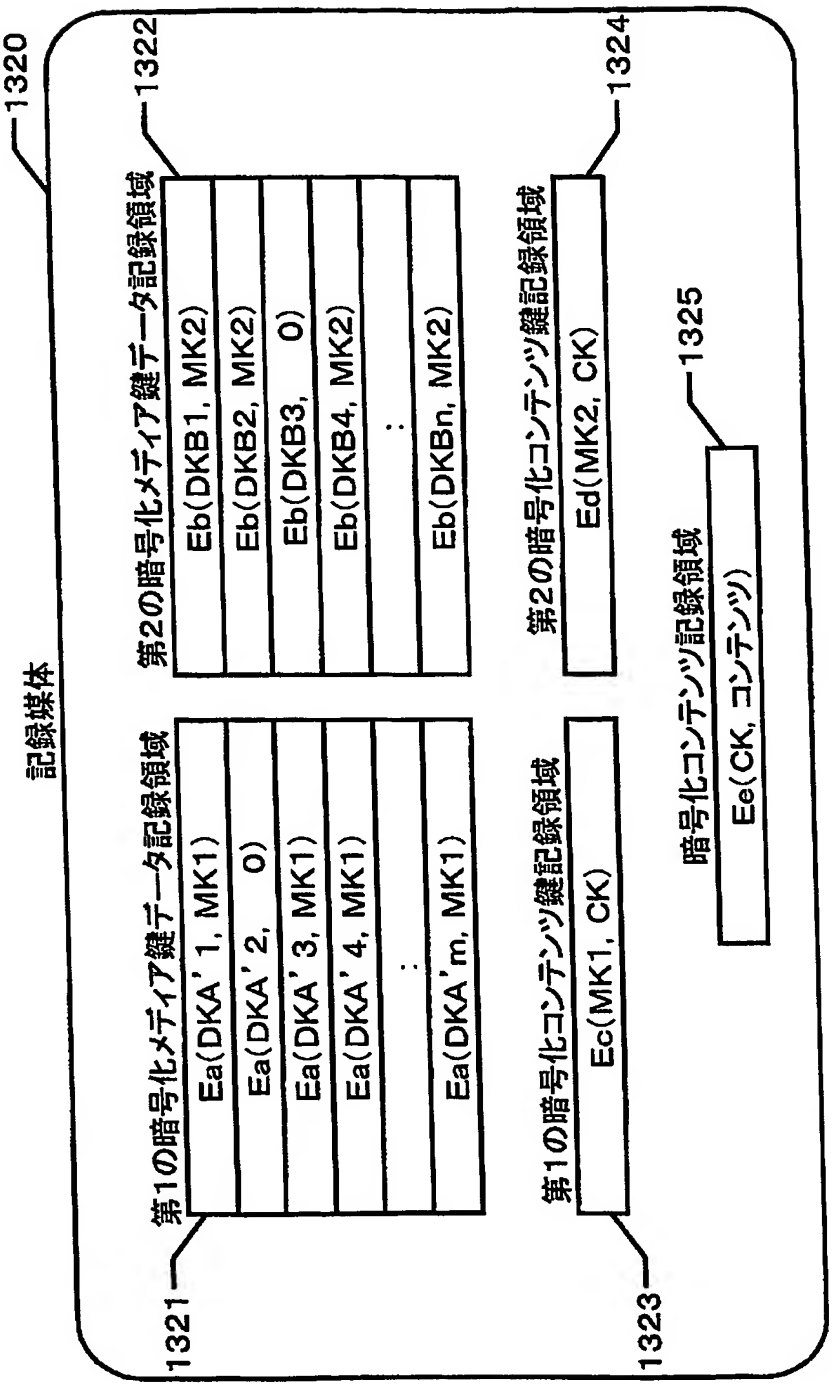
【図１６】

本発明の実施の形態3における記録媒体に記録するデータの具体例



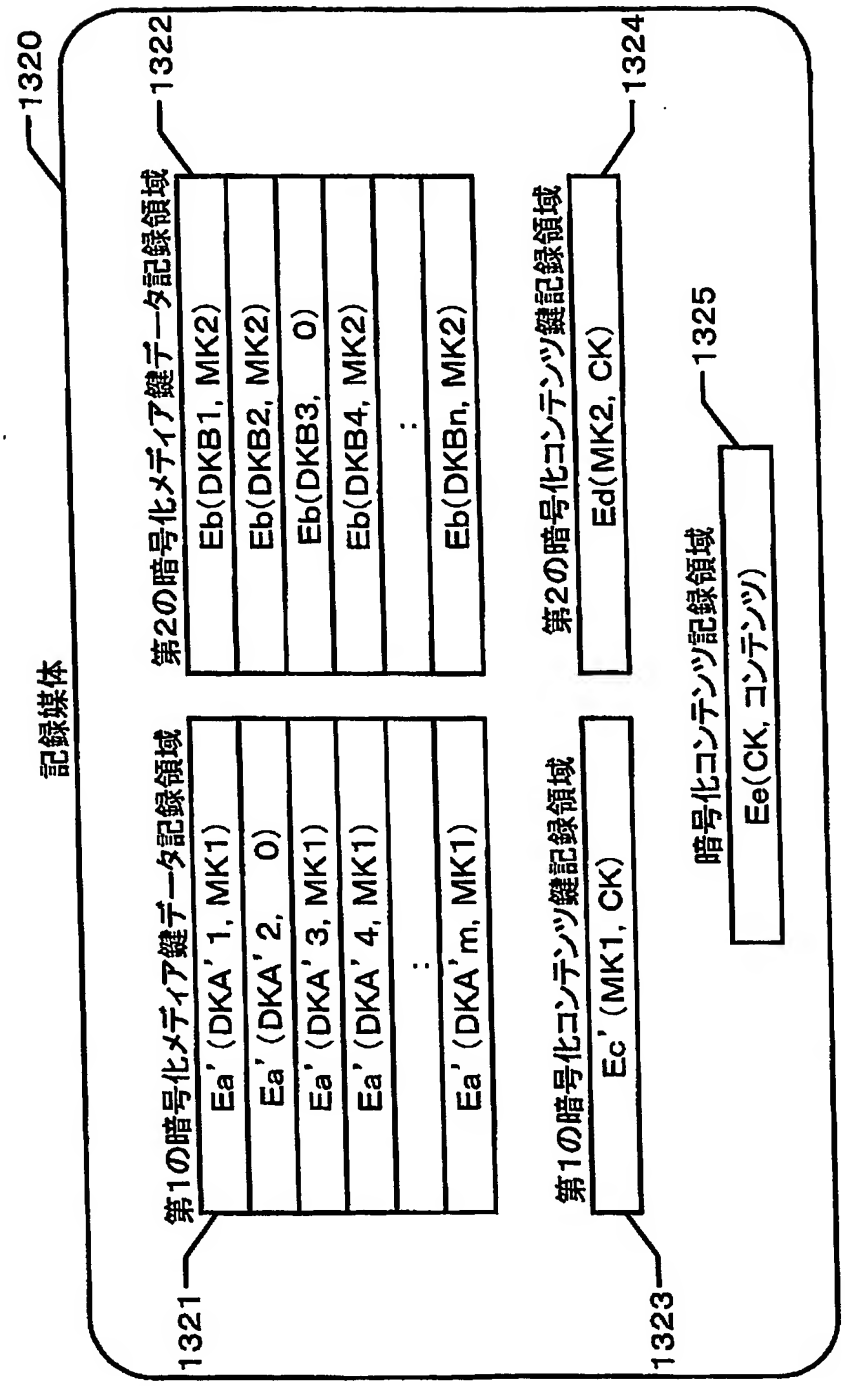
【図１７】

本発明の実施の形態3におけるシステム更新の具体例1

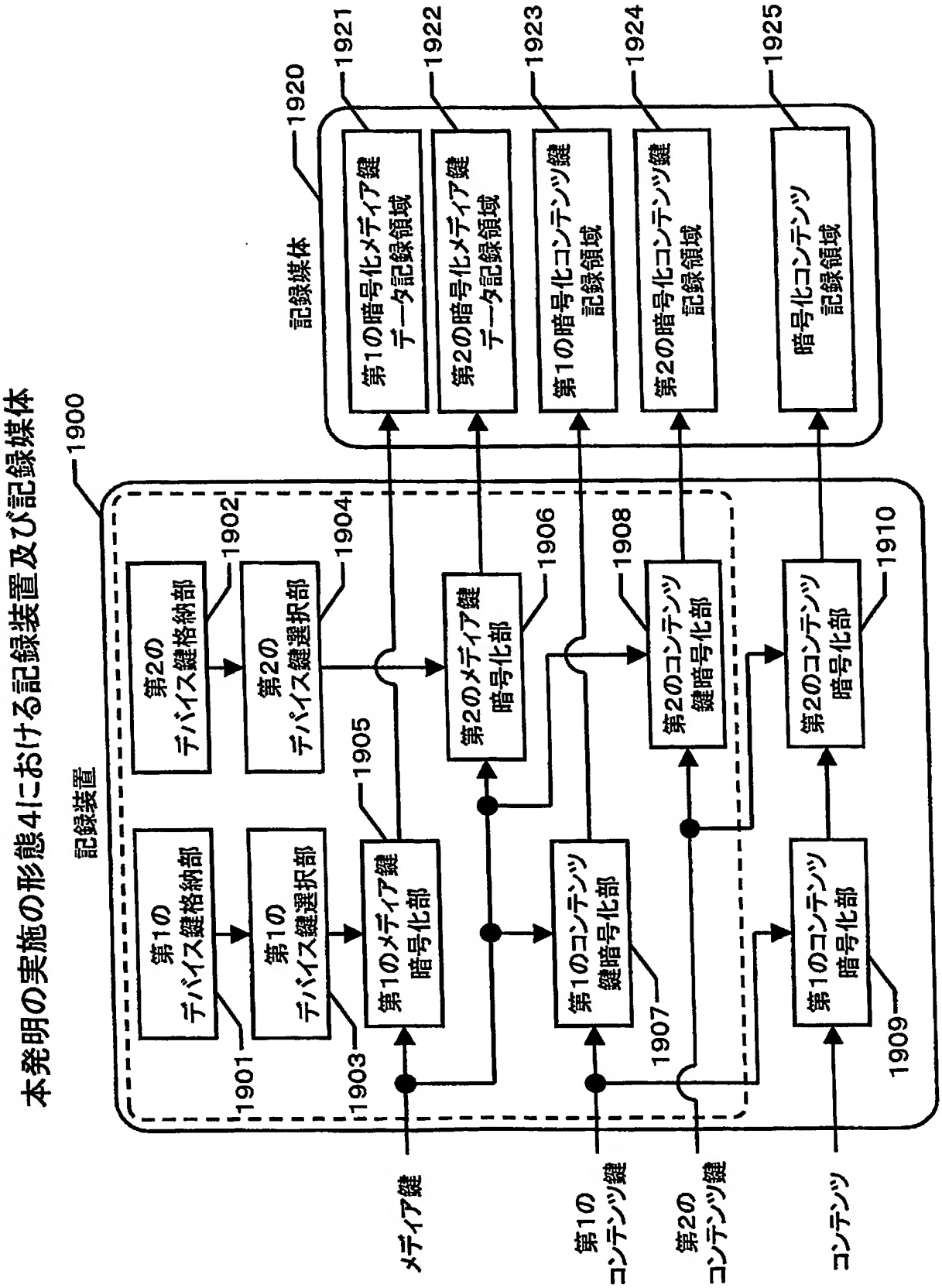


【図１８】

本発明の実施の形態3におけるシステム更新の具体例2

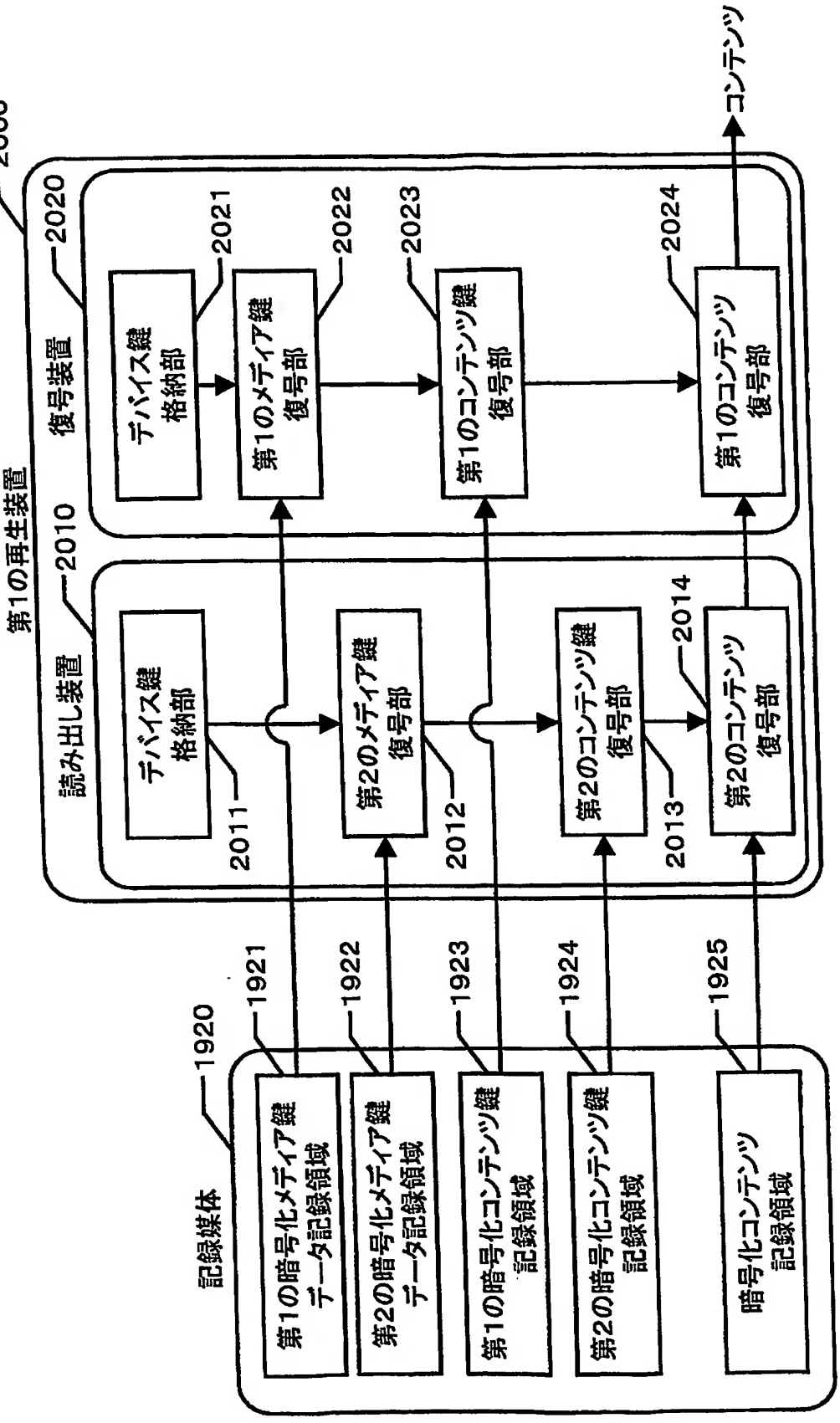


【図１９】


本発明の実施の形態4における記録装置及び記録媒体
記録装置
1900
第1の
デバイス鍵格納部
1901
第2の
デバイス鍵格納部
1902
第1の
デバイス鍵選択部
1903
第2の
デバイス鍵選択部
1904
第1のメディア鍵
暗号化部
1905
第2のメディア鍵
暗号化部
1906
第1のコンテンツ
鍵暗号化部
1907
第2のコンテンツ
鍵暗号化部
1908
第1のコンテンツ
暗号化部
1909
第2のコンテンツ
暗号化部
1910
メディア鍵
第1の
コンテンツ鍵
第2の
コンテンツ鍵
コンテンツ
記録媒体
1920
第1の暗号化メディア鍵
データ記録領域
1921
第2の暗号化メディア鍵
データ記録領域
1922
第1の暗号化コンテンツ鍵
記録領域
1923
第2の暗号化コンテンツ鍵
記録領域
1924
暗号化コンテンツ
記録領域
1925

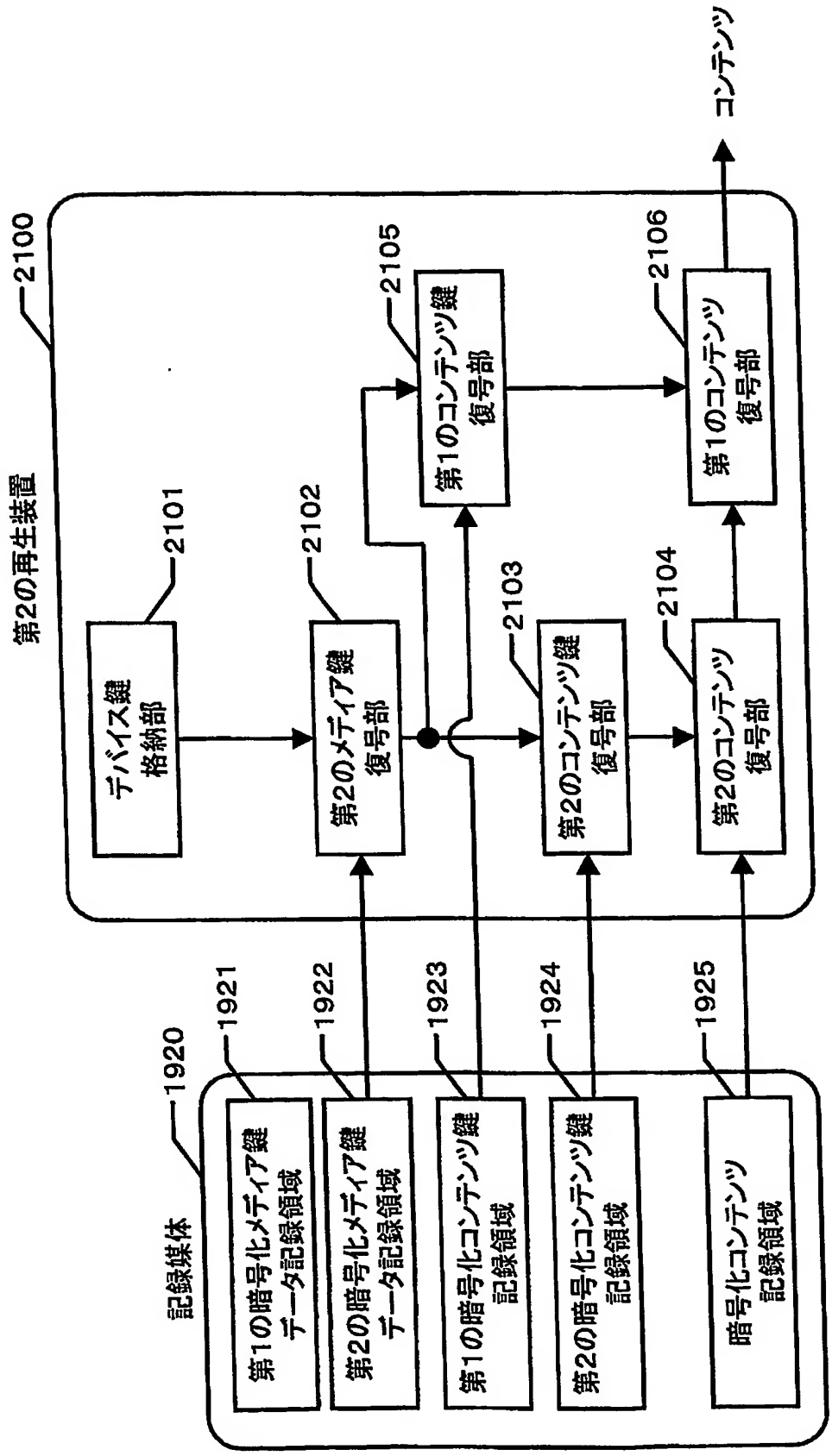
【図２０】

本発明の実施の形態4における記録媒体及び第1の再生装置



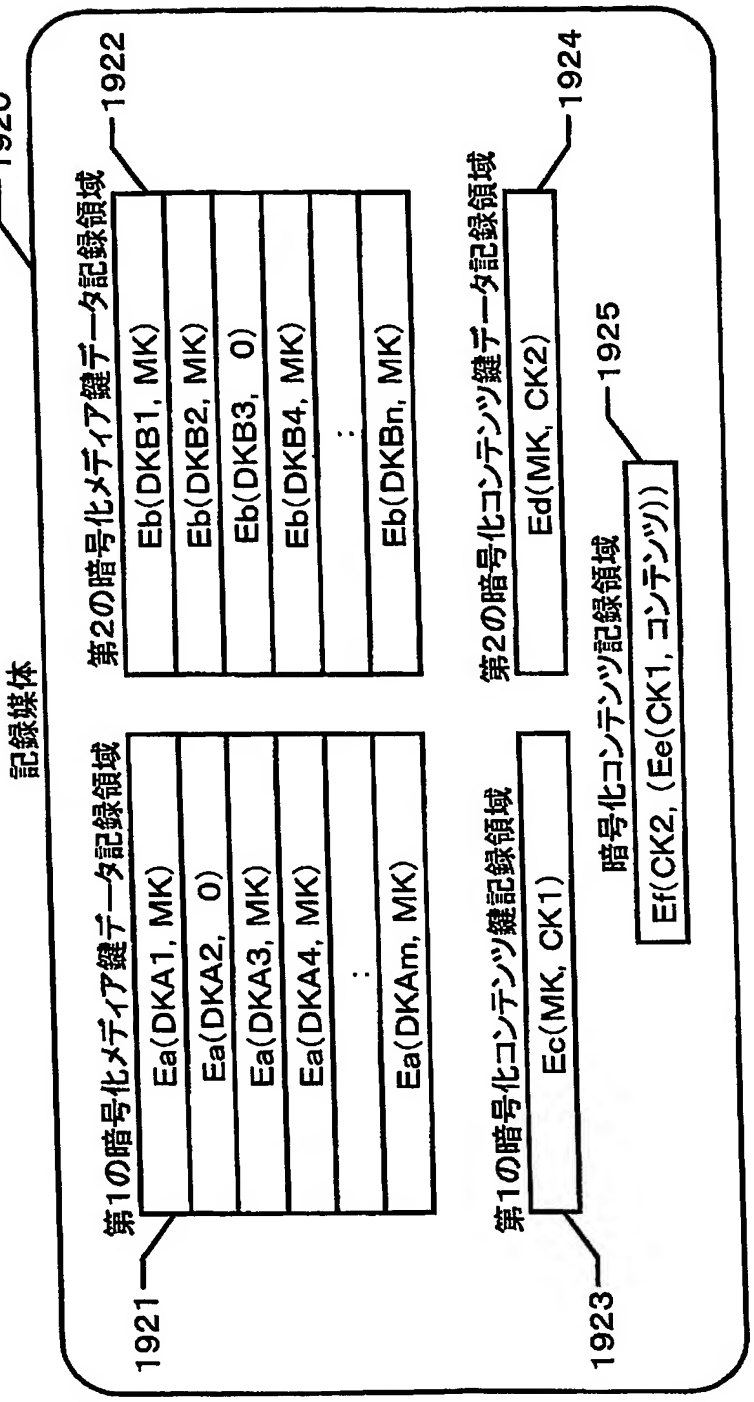
【図２１】

本発明の実施の形態4における記録媒体及び第2の再生装置



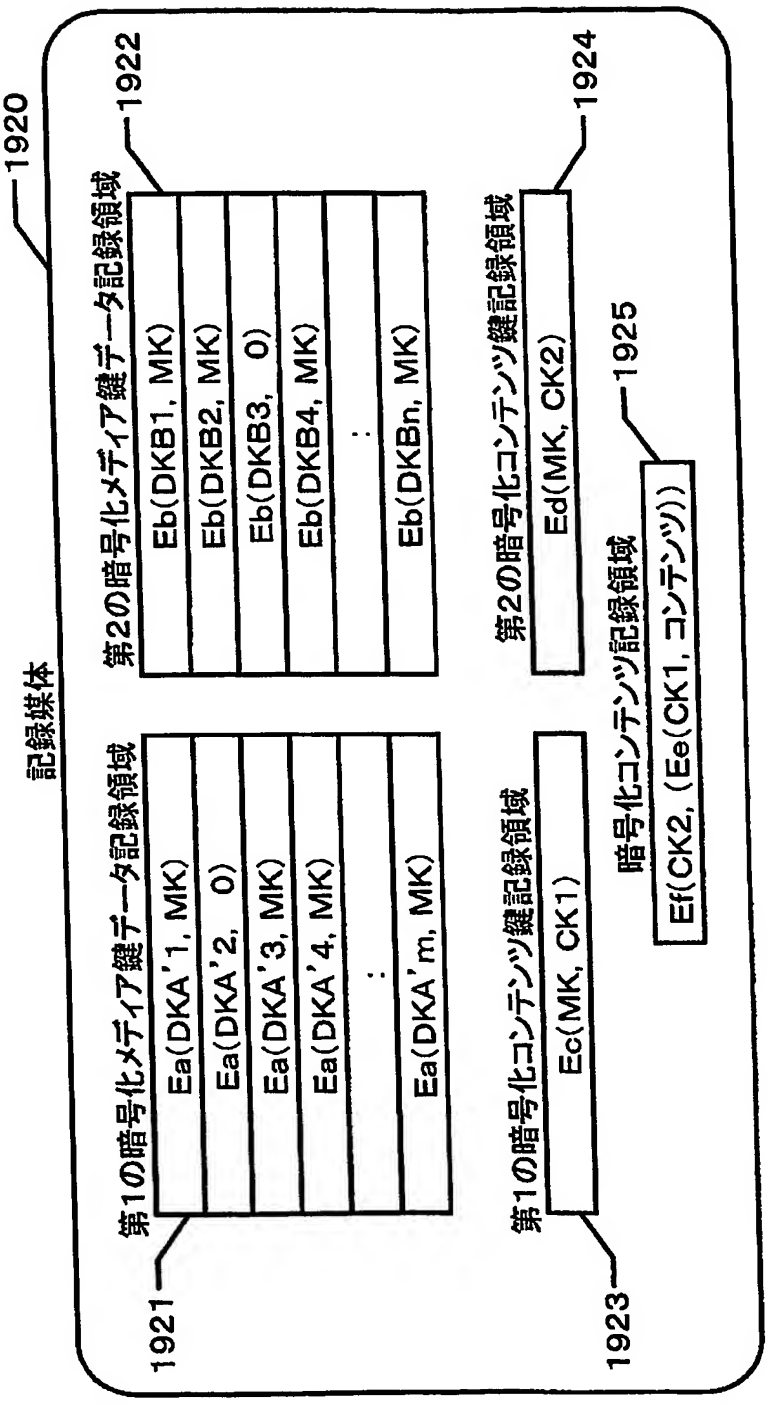
【図２２】

本発明の実施の形態4における記録媒体に記録するデータの具体例



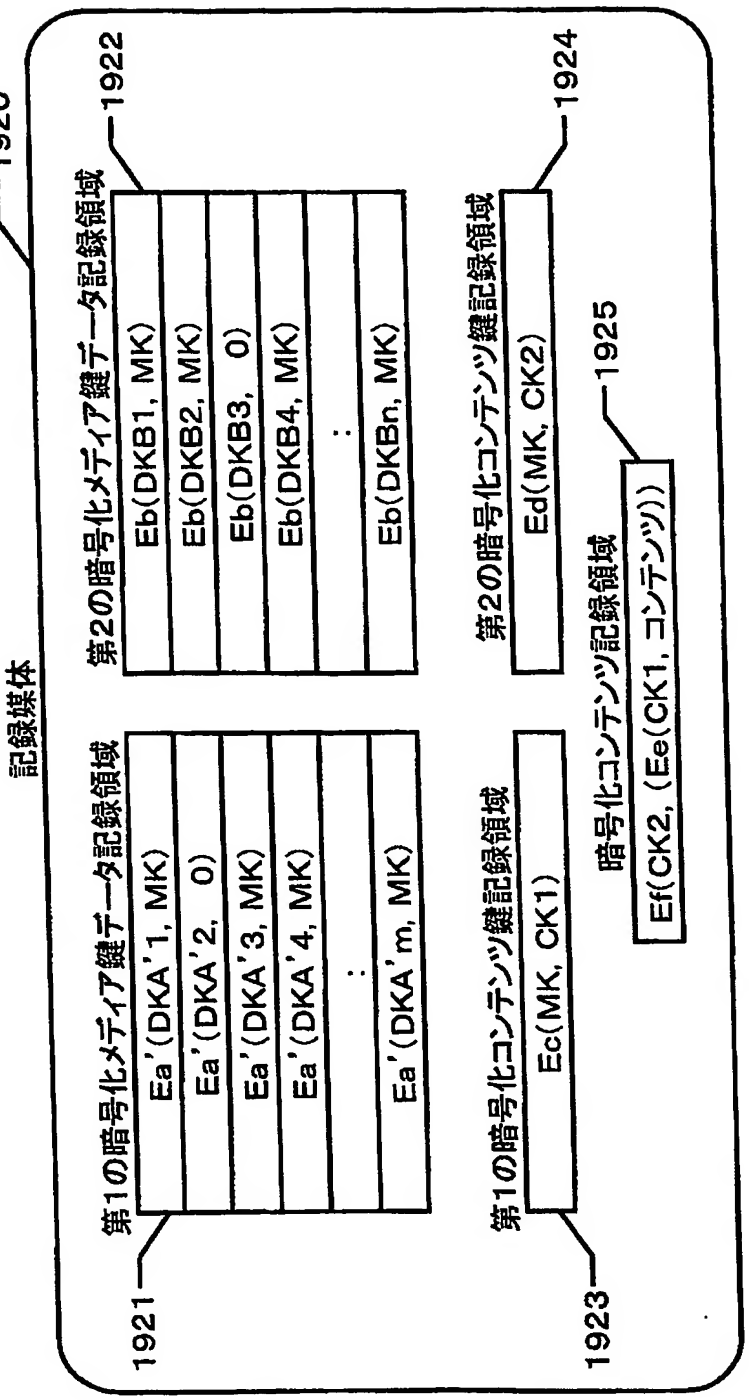
【図２３】

本発明の実施の形態4におけるシステム更新の具体例1

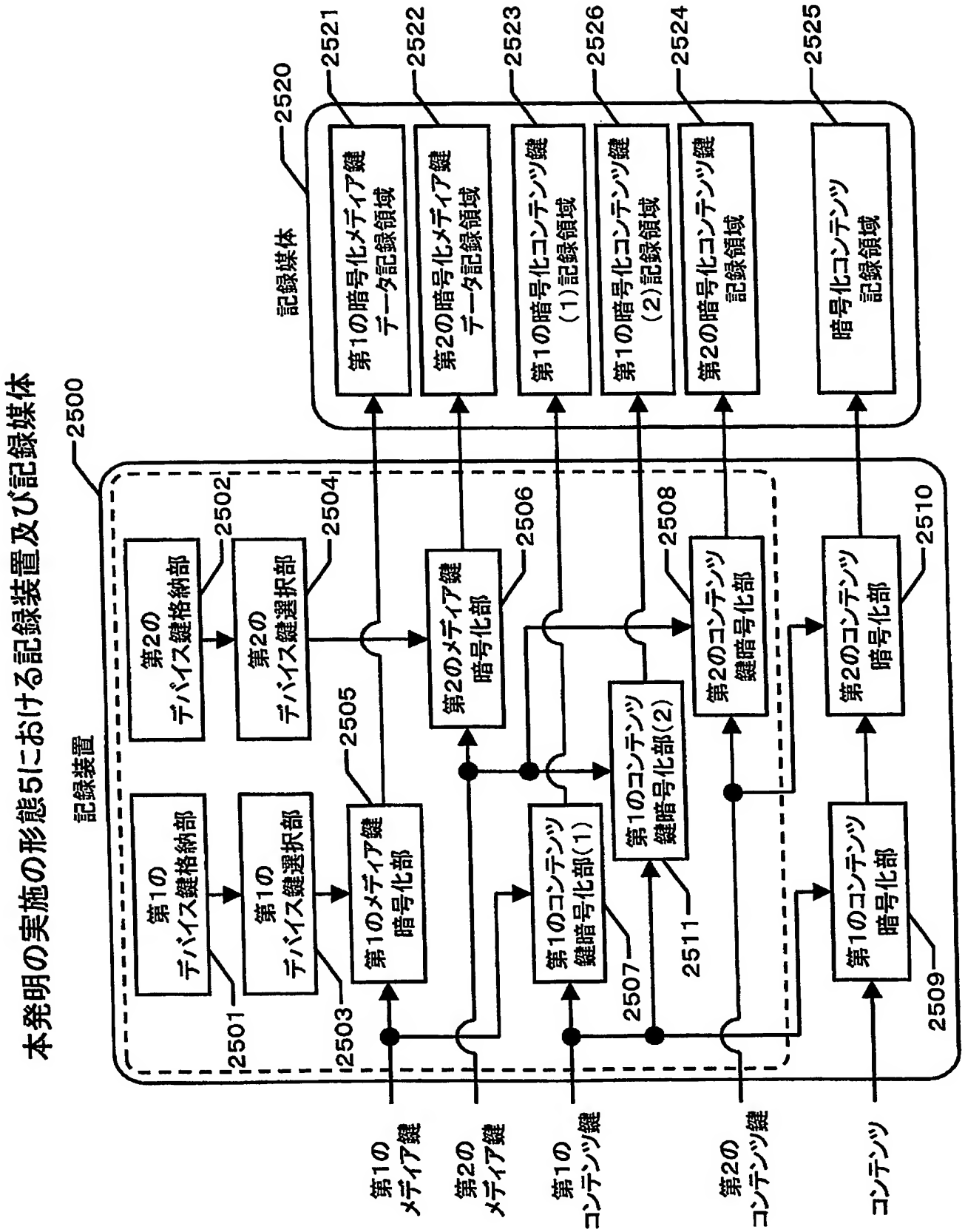


【図２４】

本発明の実施の形態4におけるシステム更新の具体例2

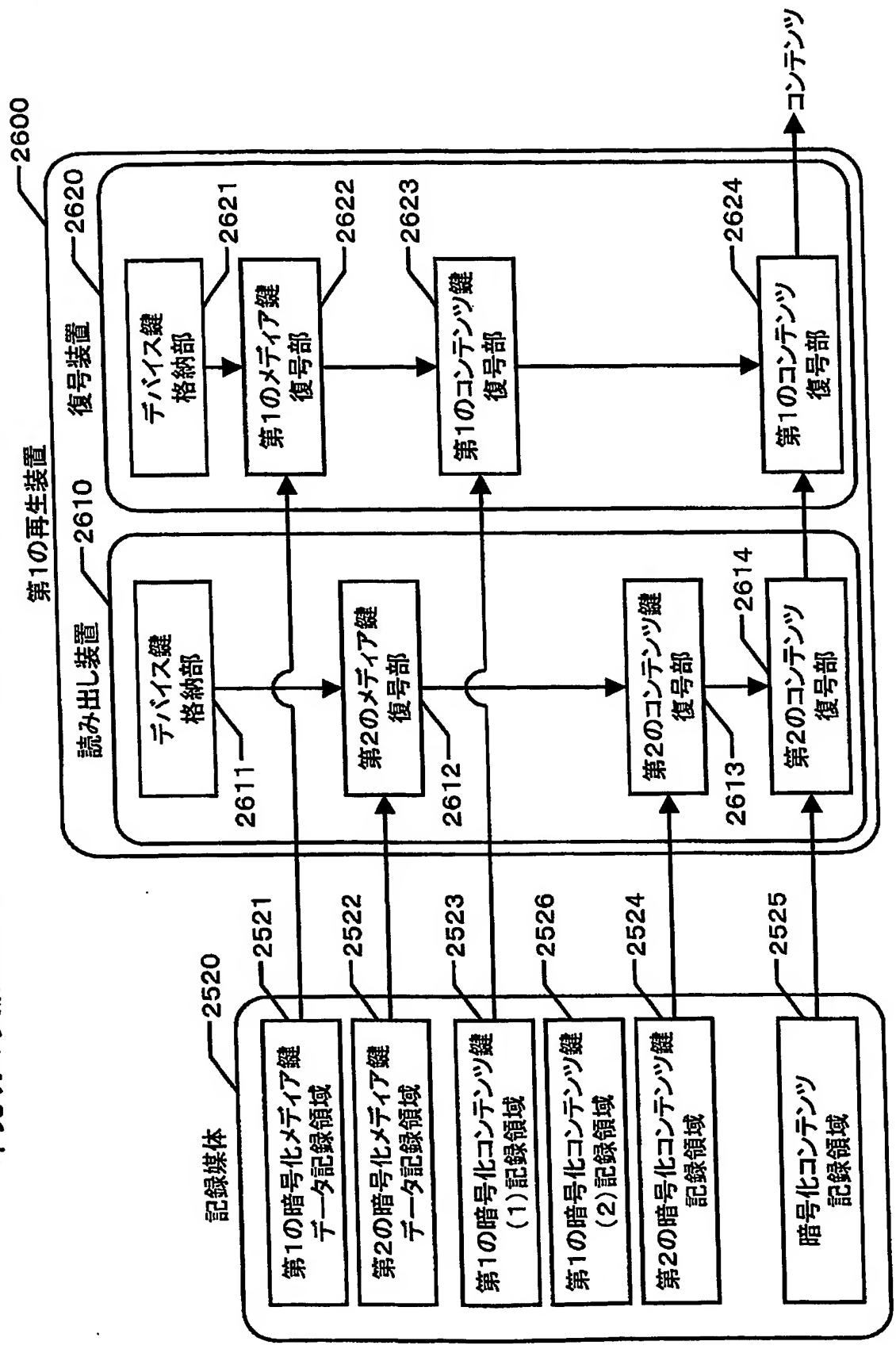


【図２５】


本発明の実施の形態5における記録装置及び記録媒体
記録装置
2500
記録媒体
2520
2521
2522
2523
2526
2524
2525
第1の暗号化メディア鍵データ記録領域
第2の暗号化メディア鍵データ記録領域
第1の暗号化コンテンツ鍵(1)記録領域
第1の暗号化コンテンツ鍵(2)記録領域
第2の暗号化コンテンツ鍵記録領域
暗号化コンテンツ記録領域
第1のデバイス鍵格納部
第2のデバイス鍵格納部
第1のデバイス鍵選択部
第2のデバイス鍵選択部
2501
2502
2503
2504
第1のメディア鍵暗号化部
第2のメディア鍵暗号化部
2505
2506
第1のコンテンツ鍵暗号化部(1)
第1のコンテンツ鍵暗号化部(2)
第2のコンテンツ鍵暗号化部
第2のコンテンツ暗号化部
2507
2508
2511
2510
第1のコンテンツ暗号化部
2509
第1のメディア鍵
第2のメディア鍵
第1のコンテンツ鍵
第2のコンテンツ鍵
コンテンツ

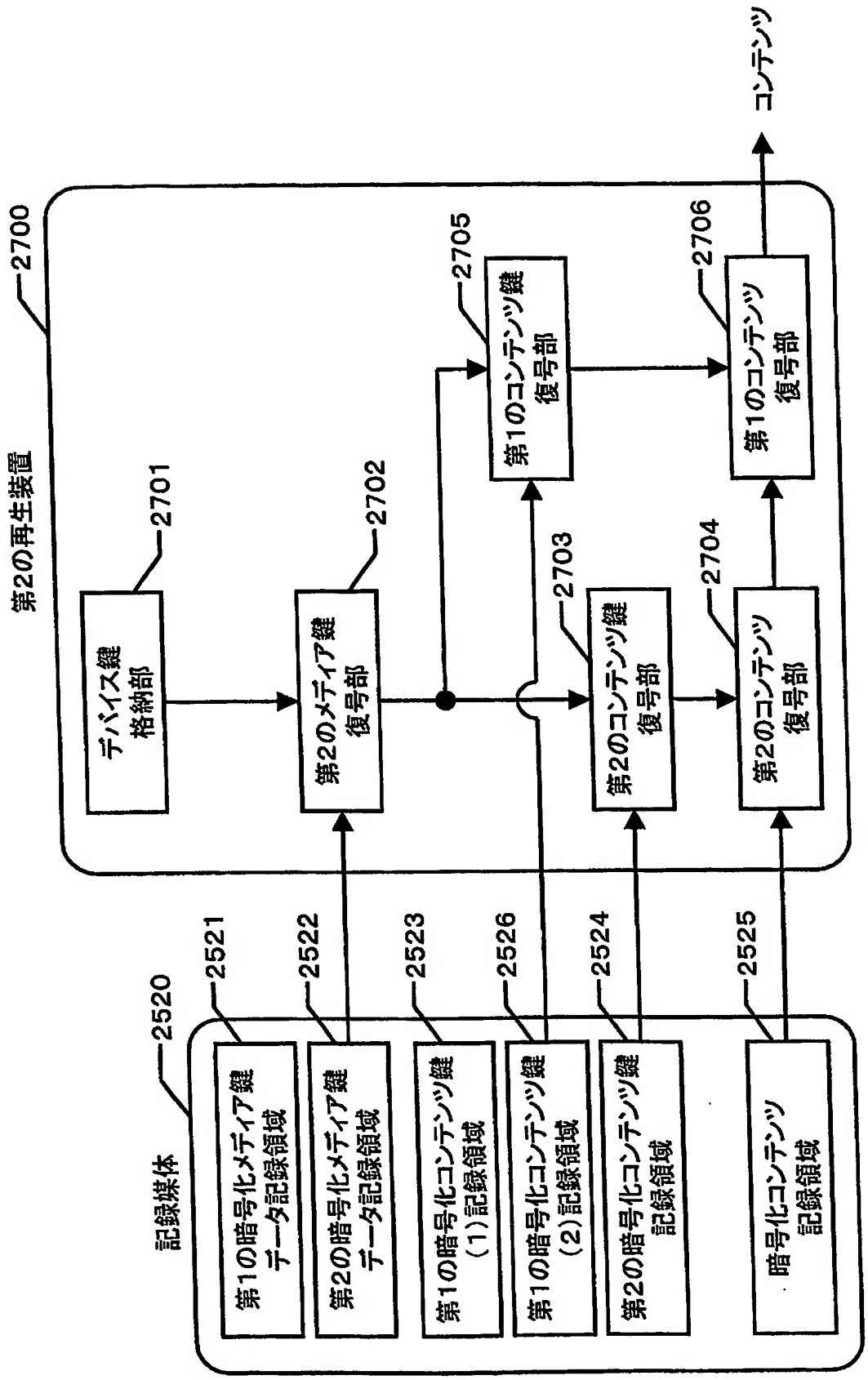
【図２６】

本発明の実施の形態5における記録媒体及び第1の再生装置



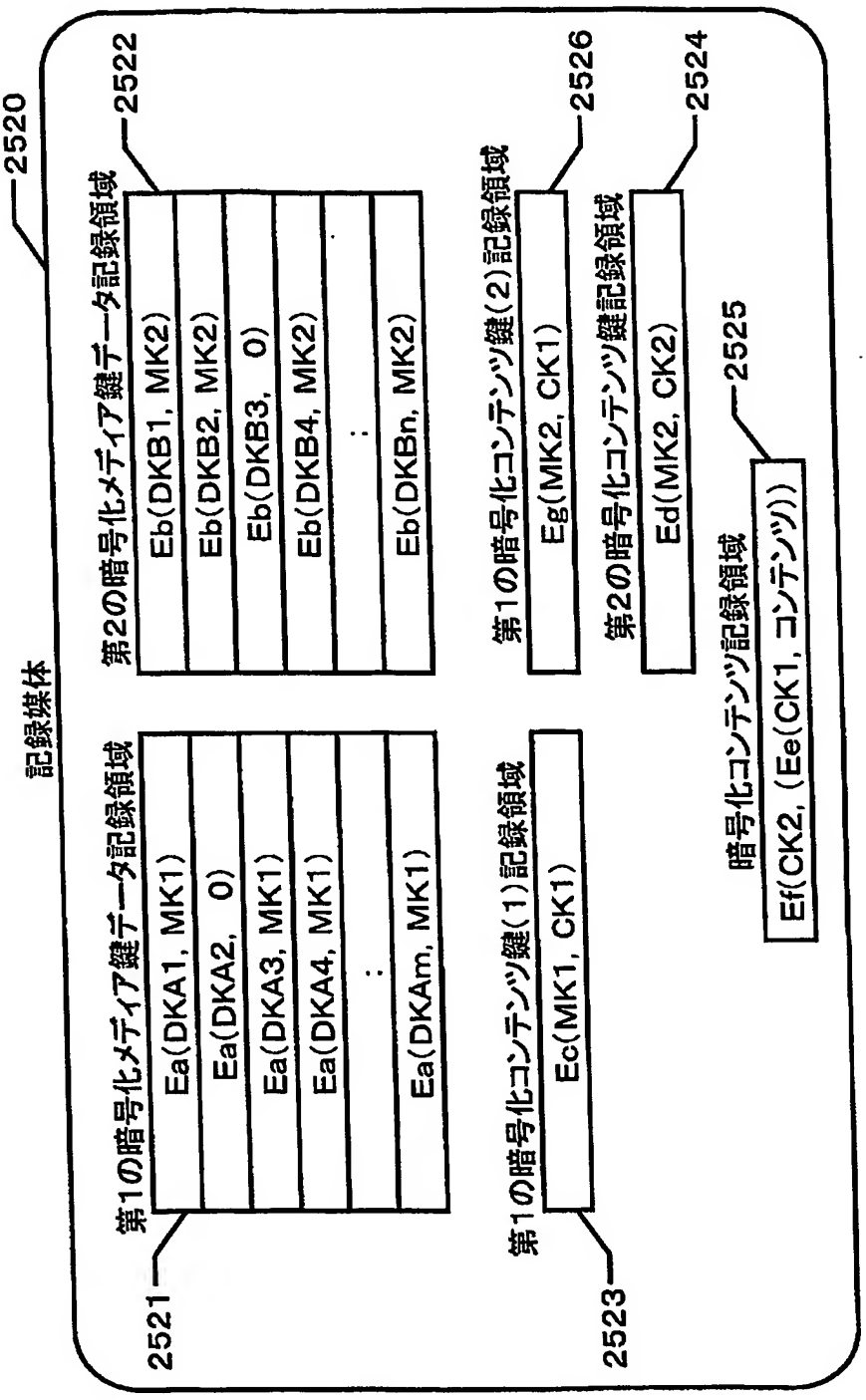
【図２７】

本発明の実施の形態5における記録媒体及び第2の再生装置



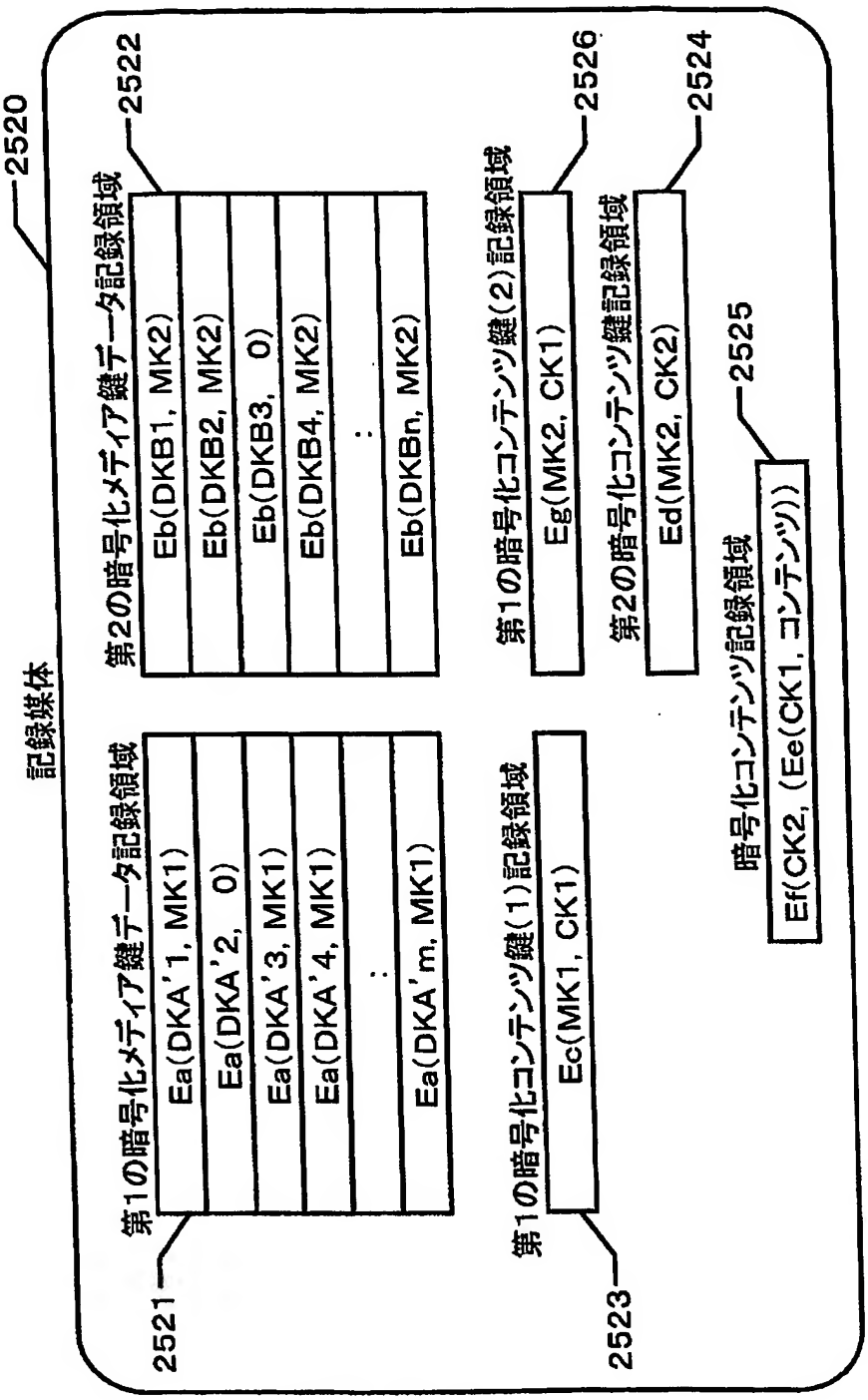
【図２８】

本発明の実施の形態5における記録媒体に記録するデータの具体例



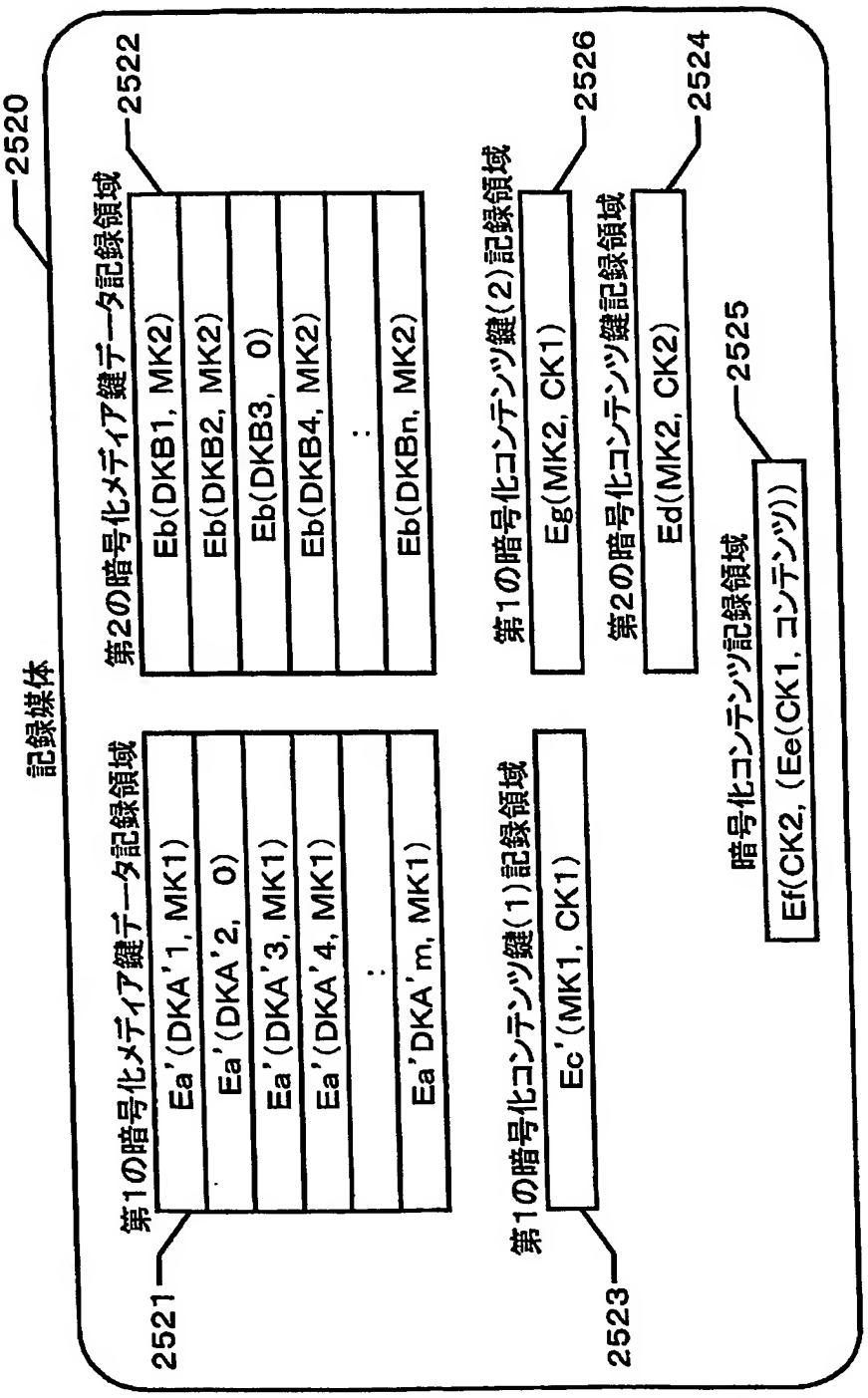
【図２９】

本発明の実施の形態5におけるシステム更新の具体例1



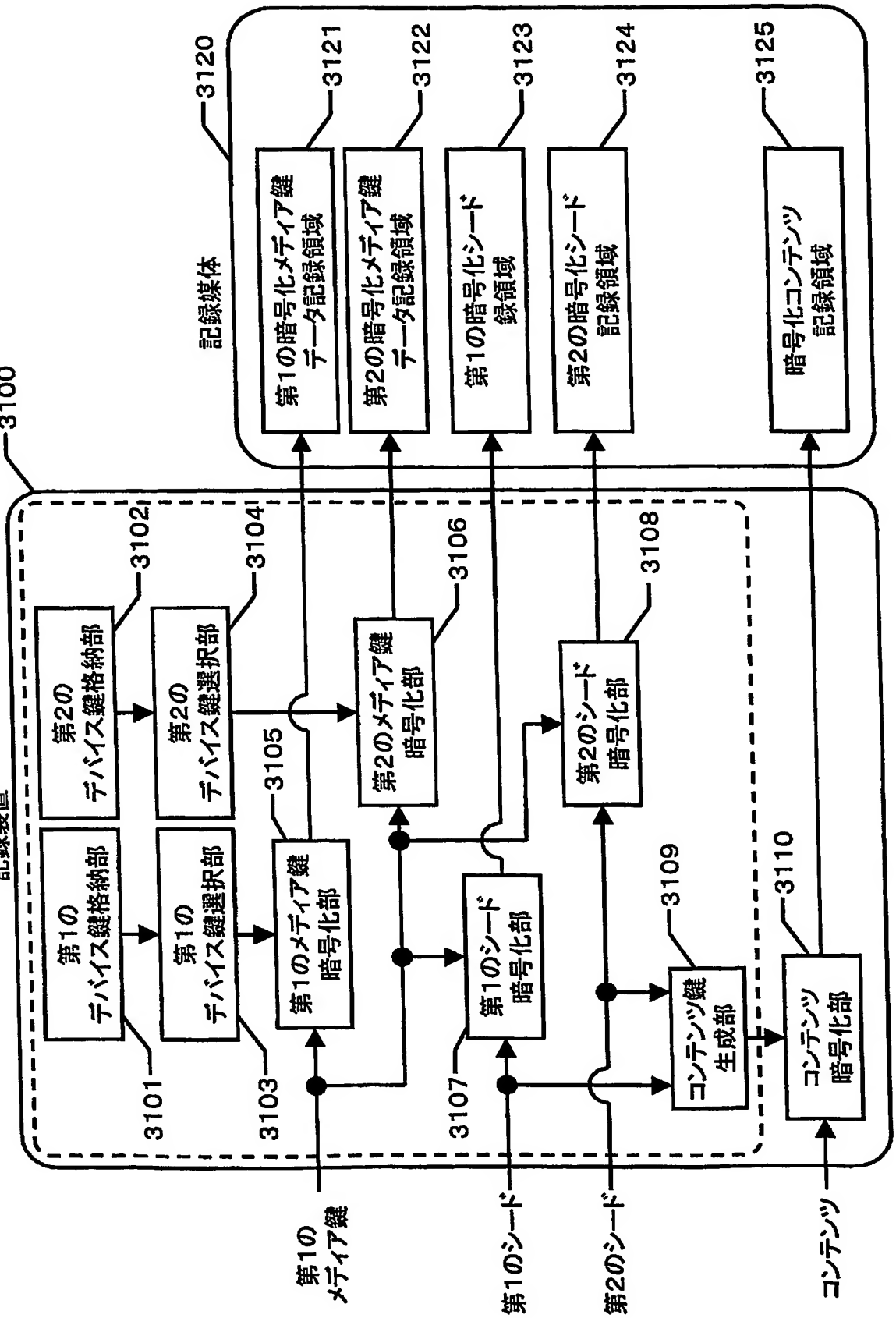
【図３０】

本発明の実施の形態5におけるシステム更新の具体例2

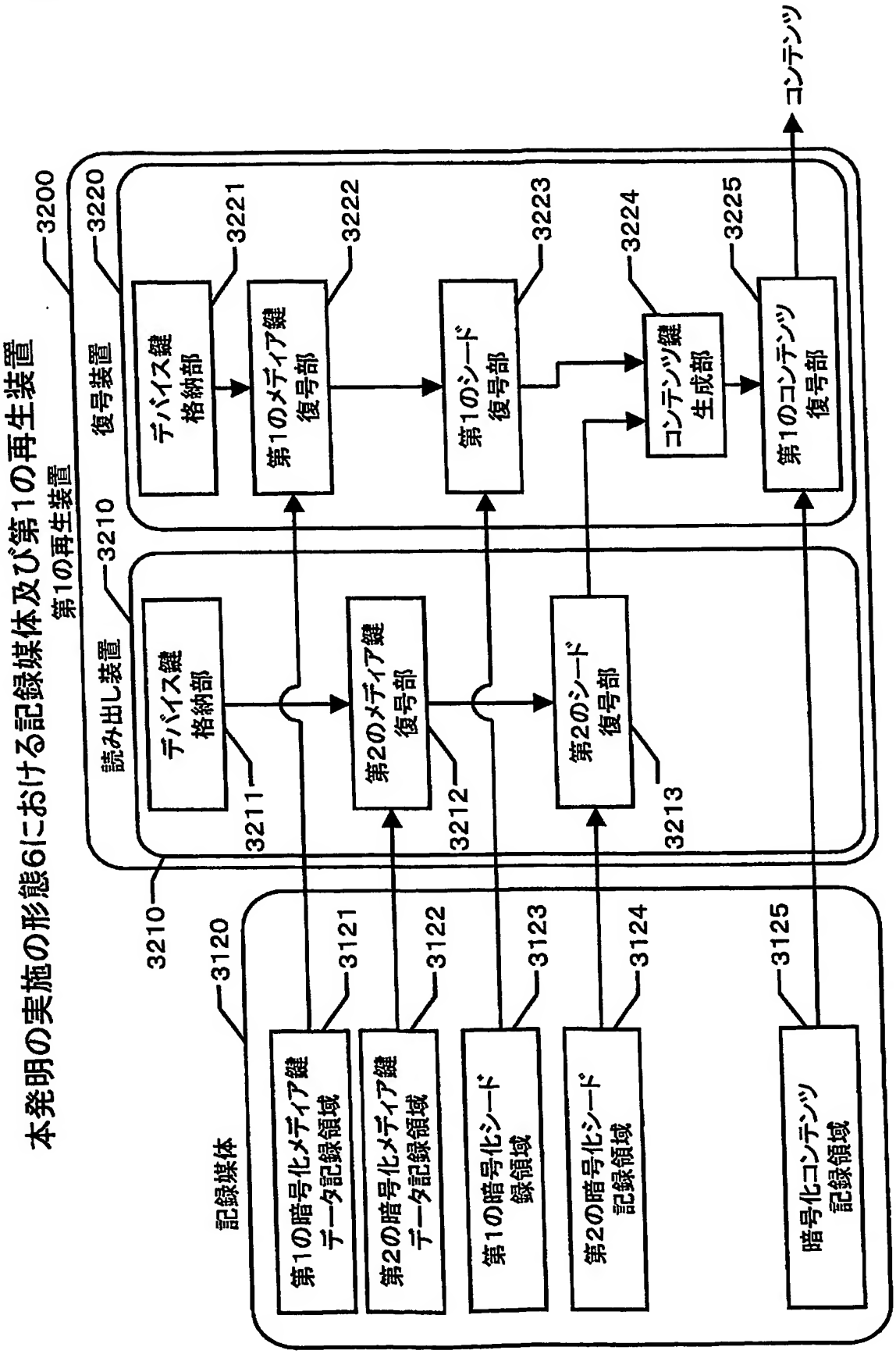


【図３１】

本発明の実施の形態6における記録装置及び記録媒体

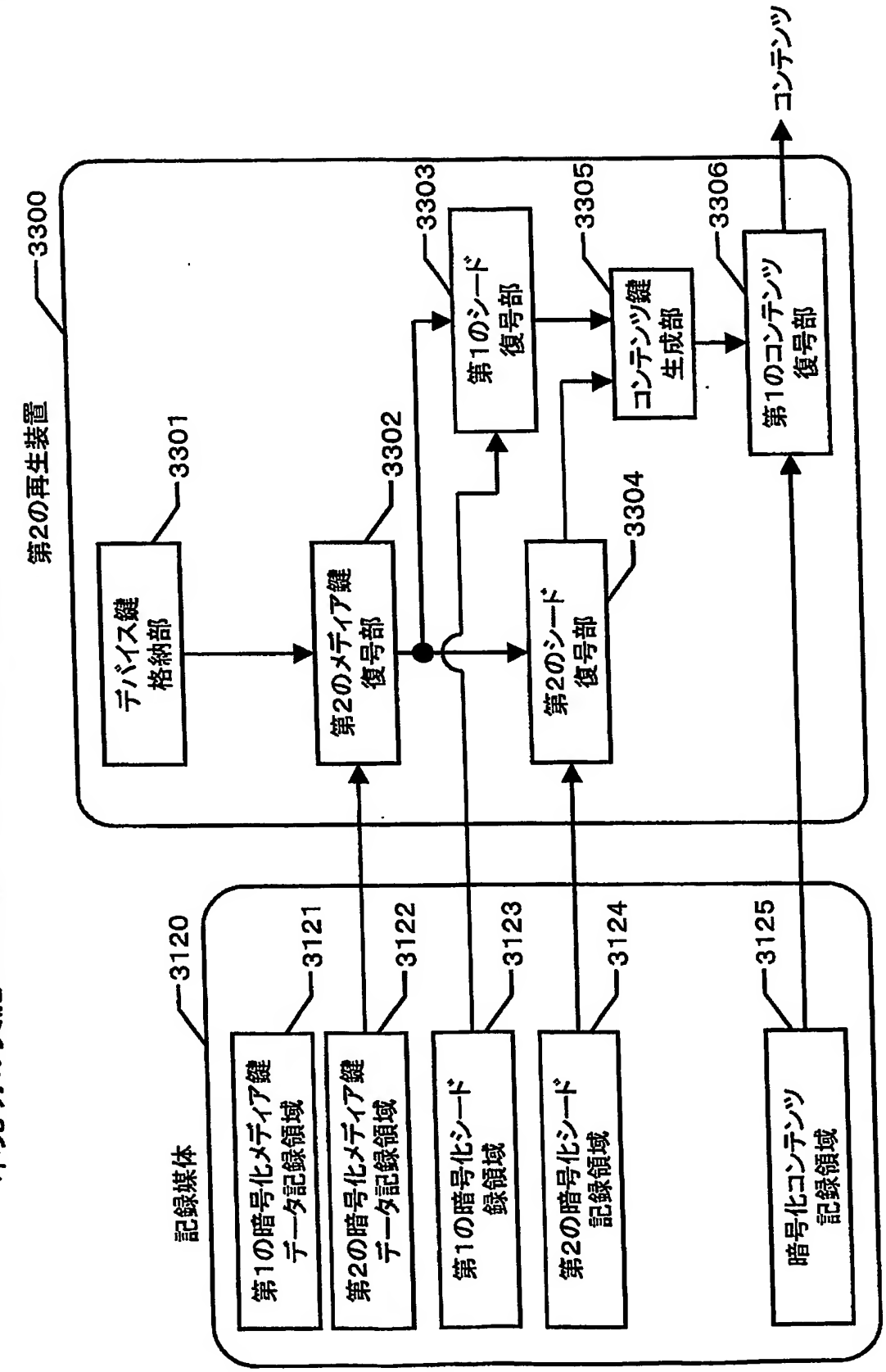


【図３２】


本発明の実施の形態6における記録媒体及び第1の再生装置
第1の再生装置
3200
3210
読み出し装置
3211
デバイス鍵格納部
3212
第2のメディア鍵復号部
3213
第2のシード復号部
3220
復号装置
3221
デバイス鍵格納部
3222
第1のメディア鍵復号部
3223
第1のシード復号部
3224
コンテンツ鍵生成部
3225
第1のコンテンツ復号部
コンテンツ
3210
3120
記録媒体
3121
第1の暗号化メディア鍵データ記録領域
3122
第2の暗号化メディア鍵データ記録領域
3123
第1の暗号化シード録領域
3124
第2の暗号化シード記録領域
3125
暗号化コンテンツ記録領域

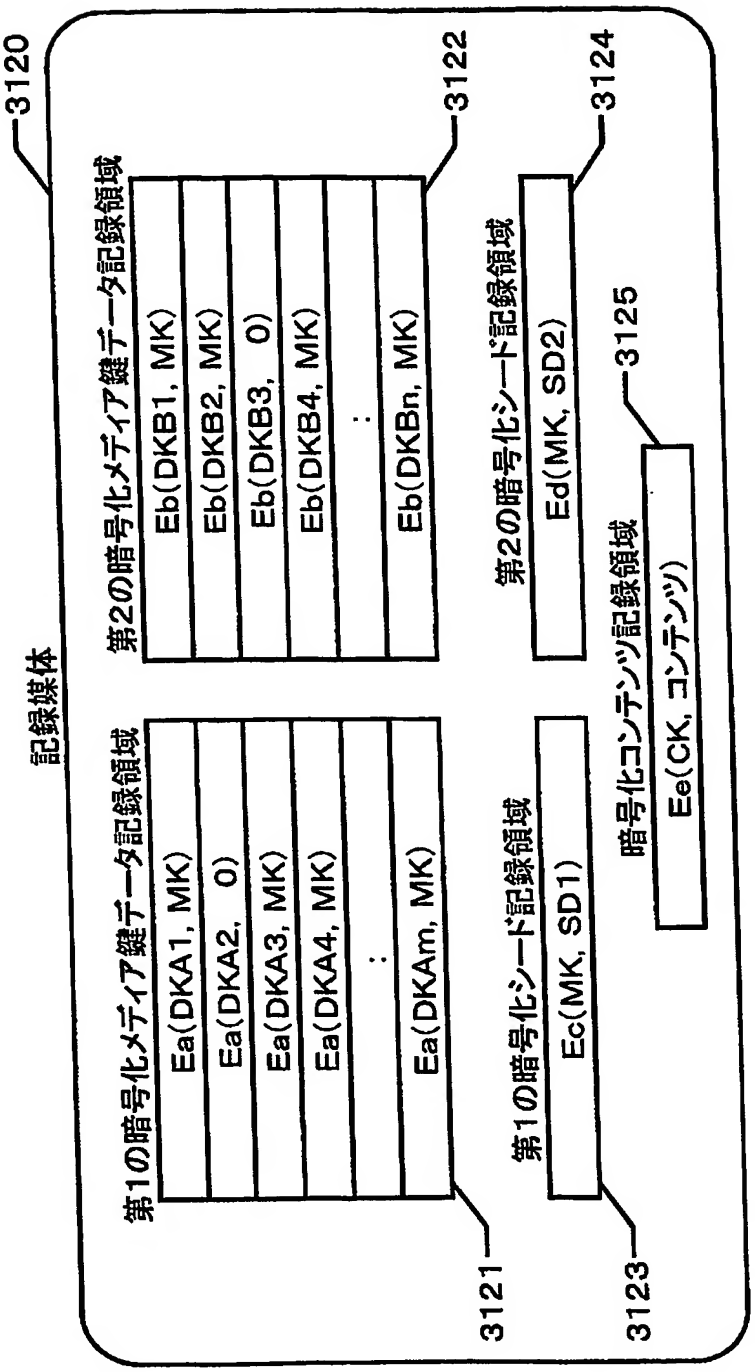
【図３３】

本発明の実施の形態6における記録媒体及び第2の再生装置



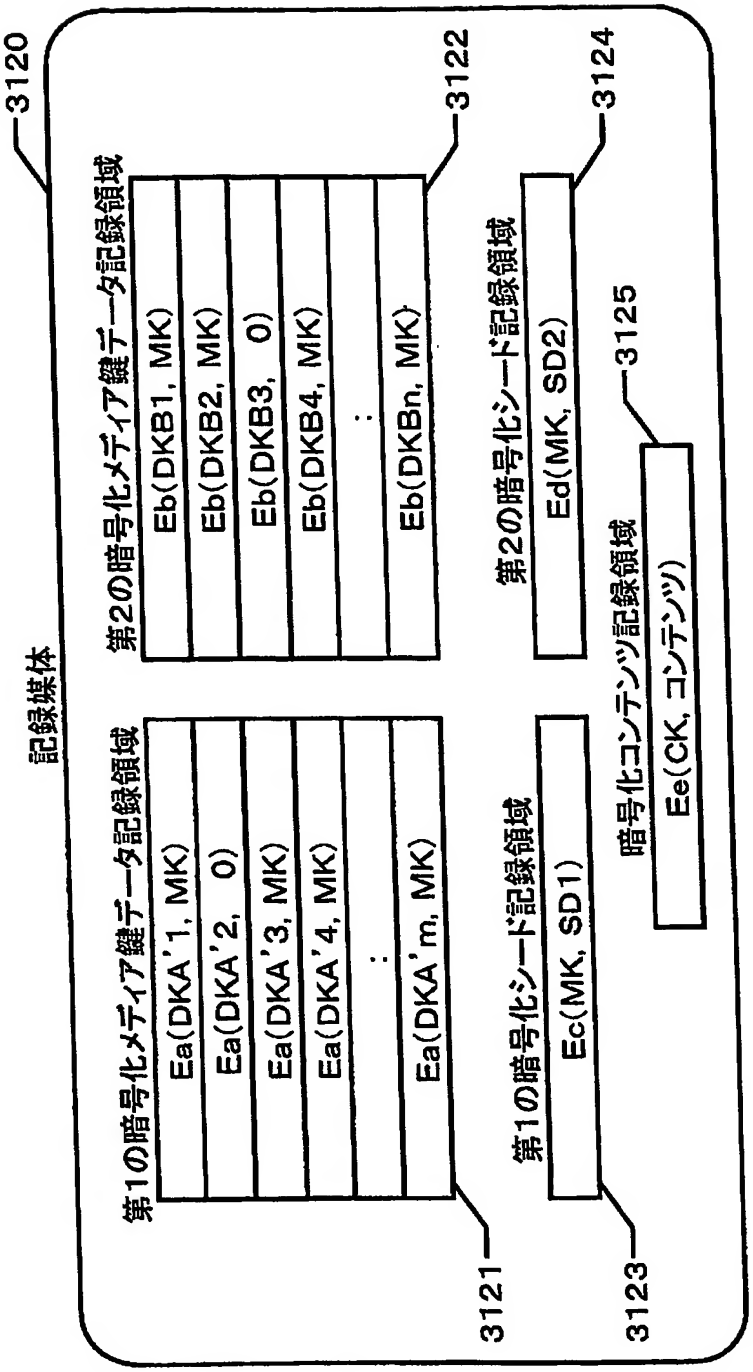
【図３４】

本発明の実施の形態6における記録媒体に記録するデータの具体例



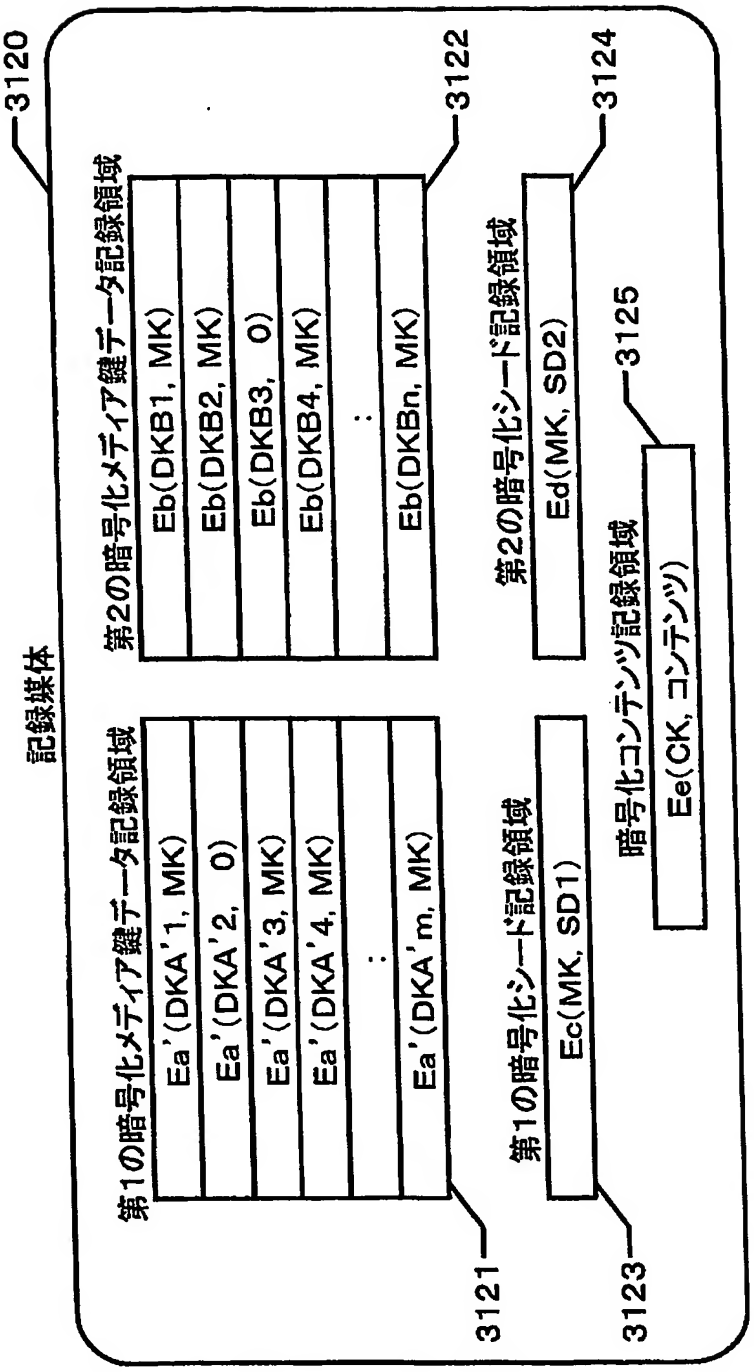
【図３５】

本発明の実施の形態6におけるシステム更新の具体例1

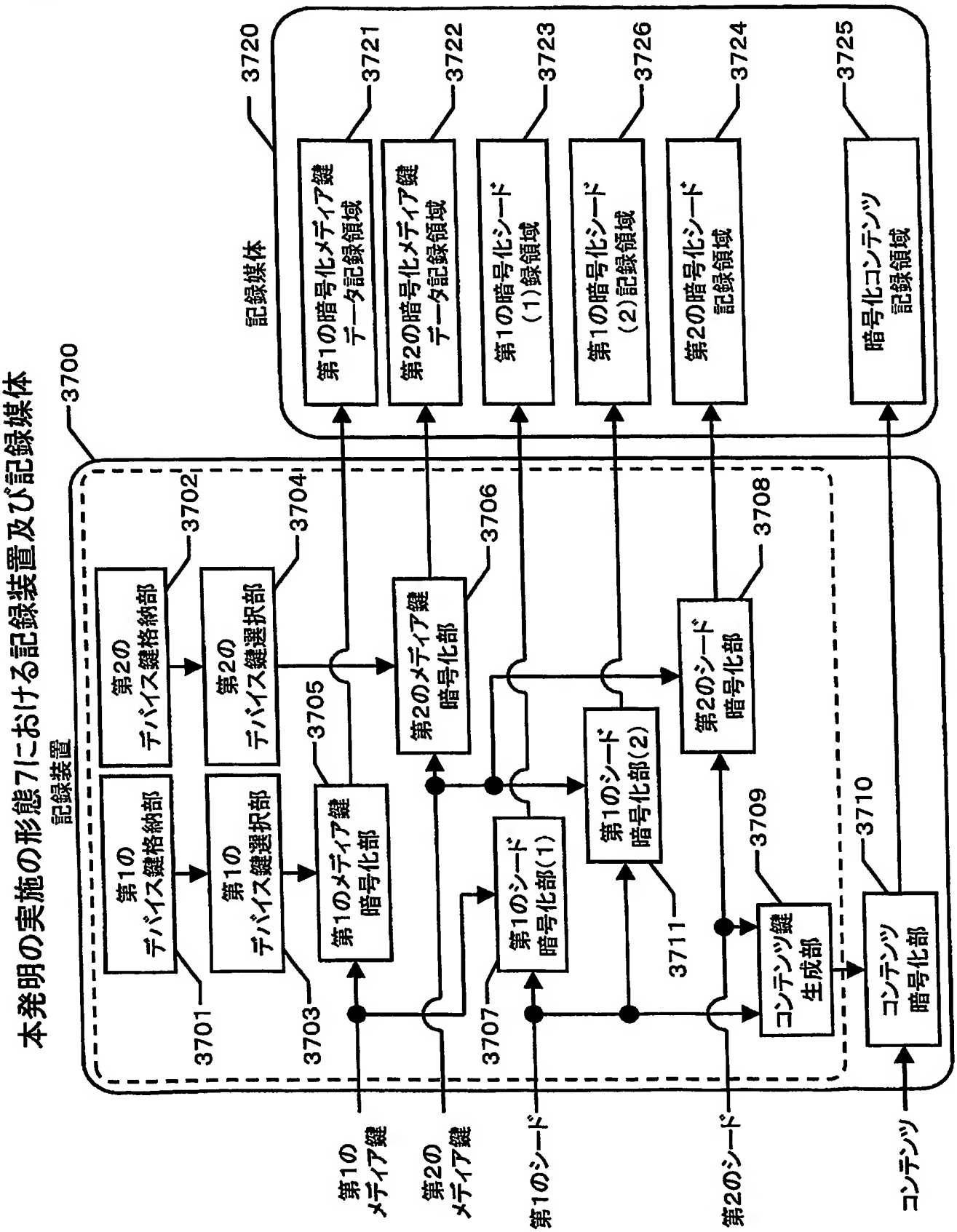


【図３６】

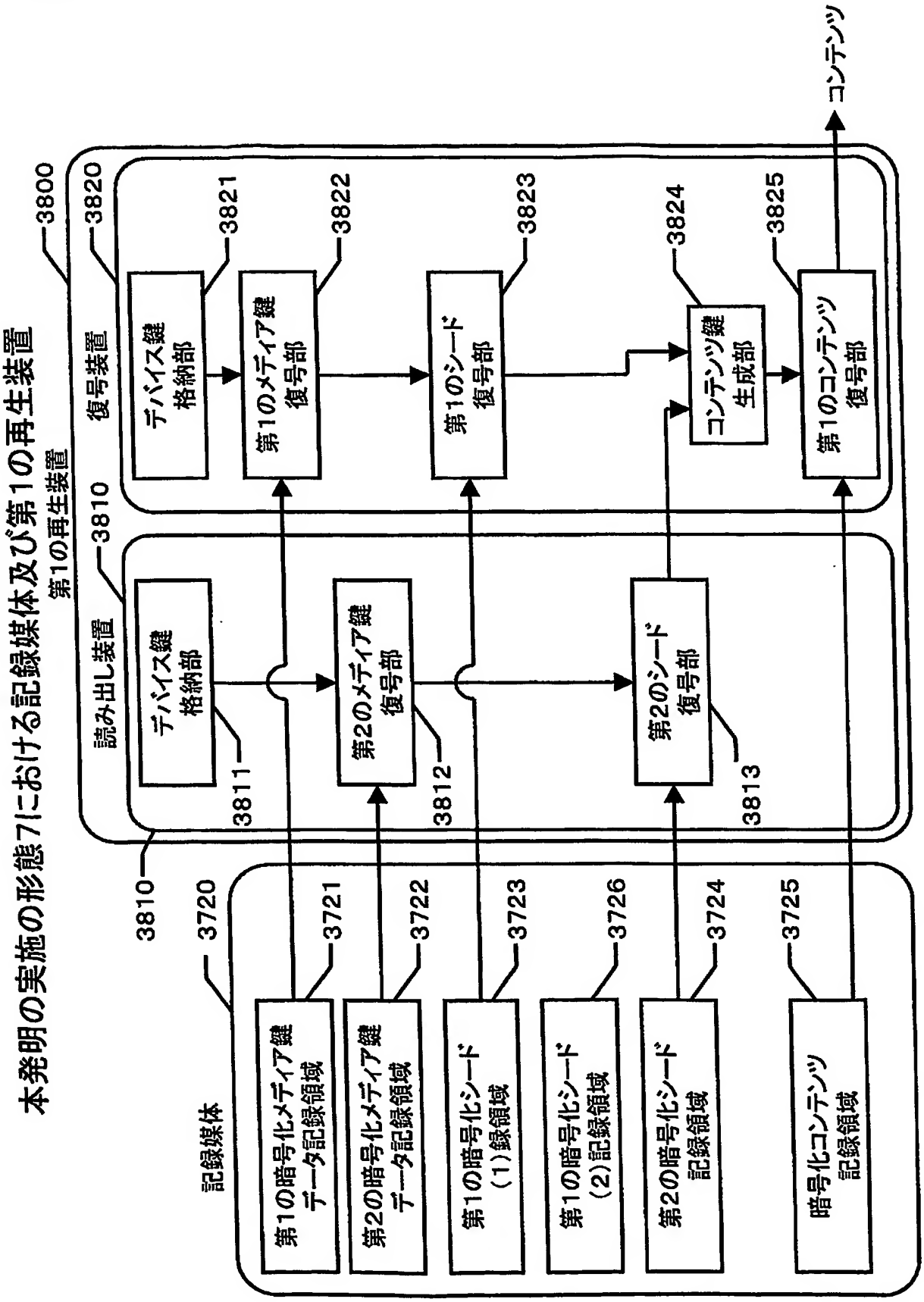
本発明の実施の形態6におけるシステム更新の具体例2



【図３７】

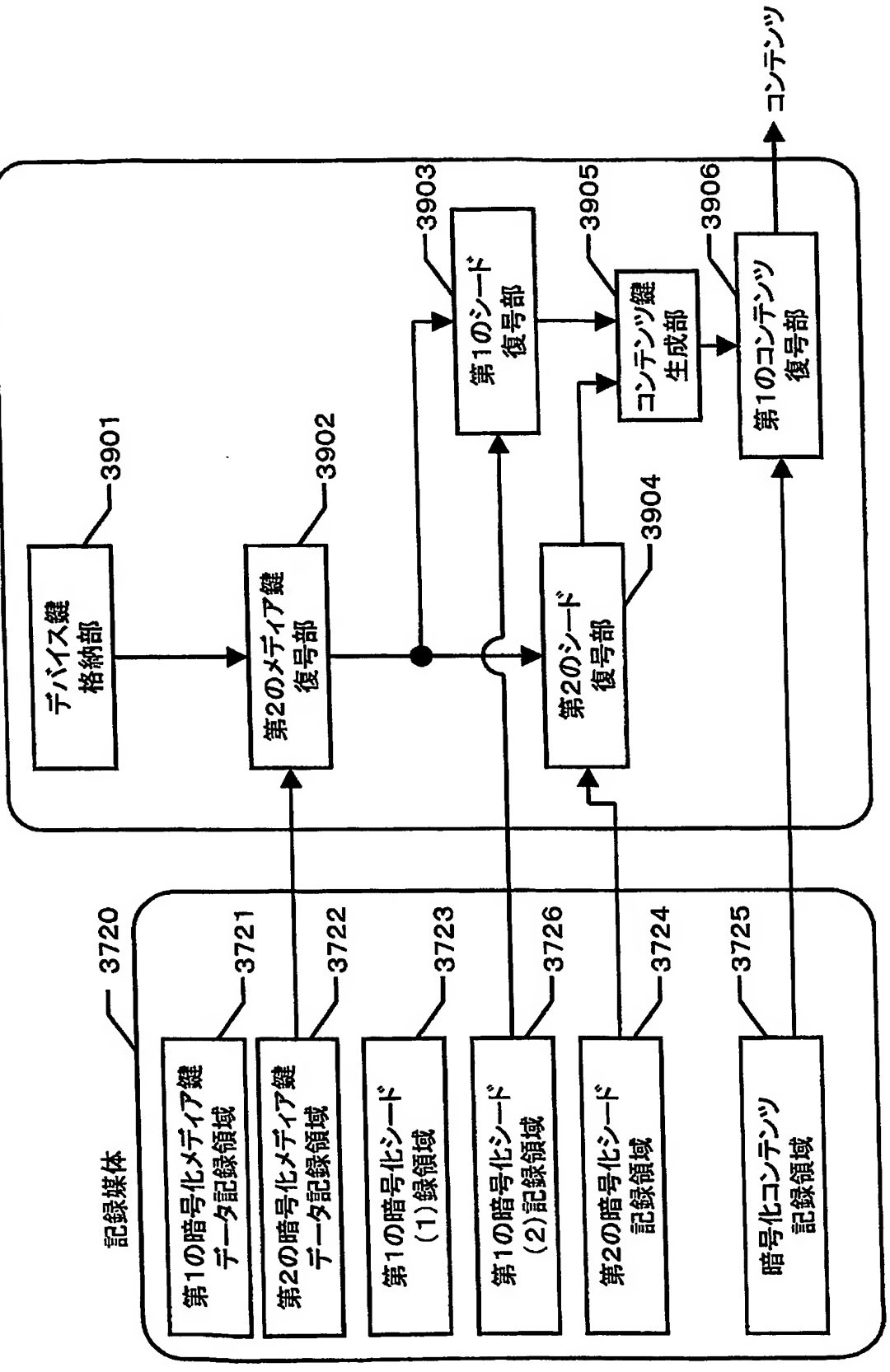

本発明の実施の形態7における記録装置及び記録媒体
記録装置
3700
記録媒体
3720
第1のデバイス鍵格納部
3701
第2のデバイス鍵格納部
3702
第1のデバイス鍵選択部
3703
第2のデバイス鍵選択部
3704
第1のメディア鍵暗号化部
3705
第2のメディア鍵暗号化部
3706
第1のシード暗号化部(1)
3707
第2のシード暗号化部
3708
コンテンツ鍵生成部
3709
コンテンツ暗号化部
3710
第1のシード暗号化部(2)
3711
第1のメディア鍵
第2のメディア鍵
第1のシード
第2のシード
コンテンツ
第1の暗号化メディア鍵データ記録領域
3721
第2の暗号化メディア鍵データ記録領域
3722
第1の暗号化シード(1)録領域
3723
第1の暗号化シード(2)記録領域
3726
第2の暗号化シード記録領域
3724
暗号化コンテンツ記録領域
3725

【図３８】


本発明の実施の形態7における記録媒体及び第1の再生装置
第1の再生装置
3800
3820
復号装置
3810
読み出し装置
デバイス鍵格納部
3821
第1のメディア鍵復号部
3822
第1のシード復号部
3823
コンテンツ鍵生成部
3824
第1のコンテンツ復号部
3825
コンテンツ
デバイス鍵格納部
3811
第2のメディア鍵復号部
3812
第2のシード復号部
3813
3810
記録媒体
3720
第1の暗号化メディア鍵データ記録領域
3721
第2の暗号化メディア鍵データ記録領域
3722
第1の暗号化シード(1)録領域
3723
第1の暗号化シード(2)記録領域
3726
第2の暗号化シード記録領域
3724
暗号化コンテンツ記録領域
3725

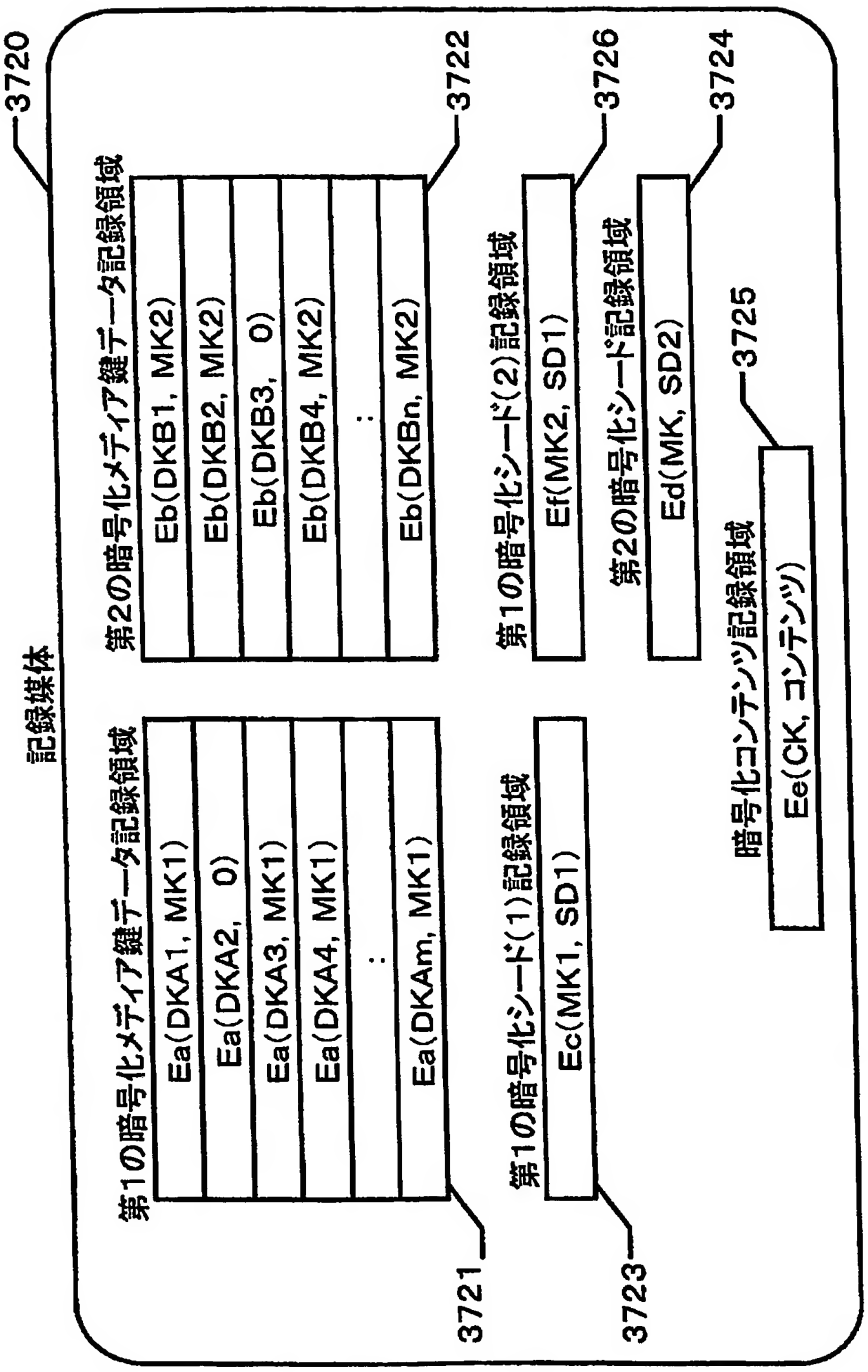
【図３９】

本発明の実施の形態7における記録媒体及び第2の再生装置



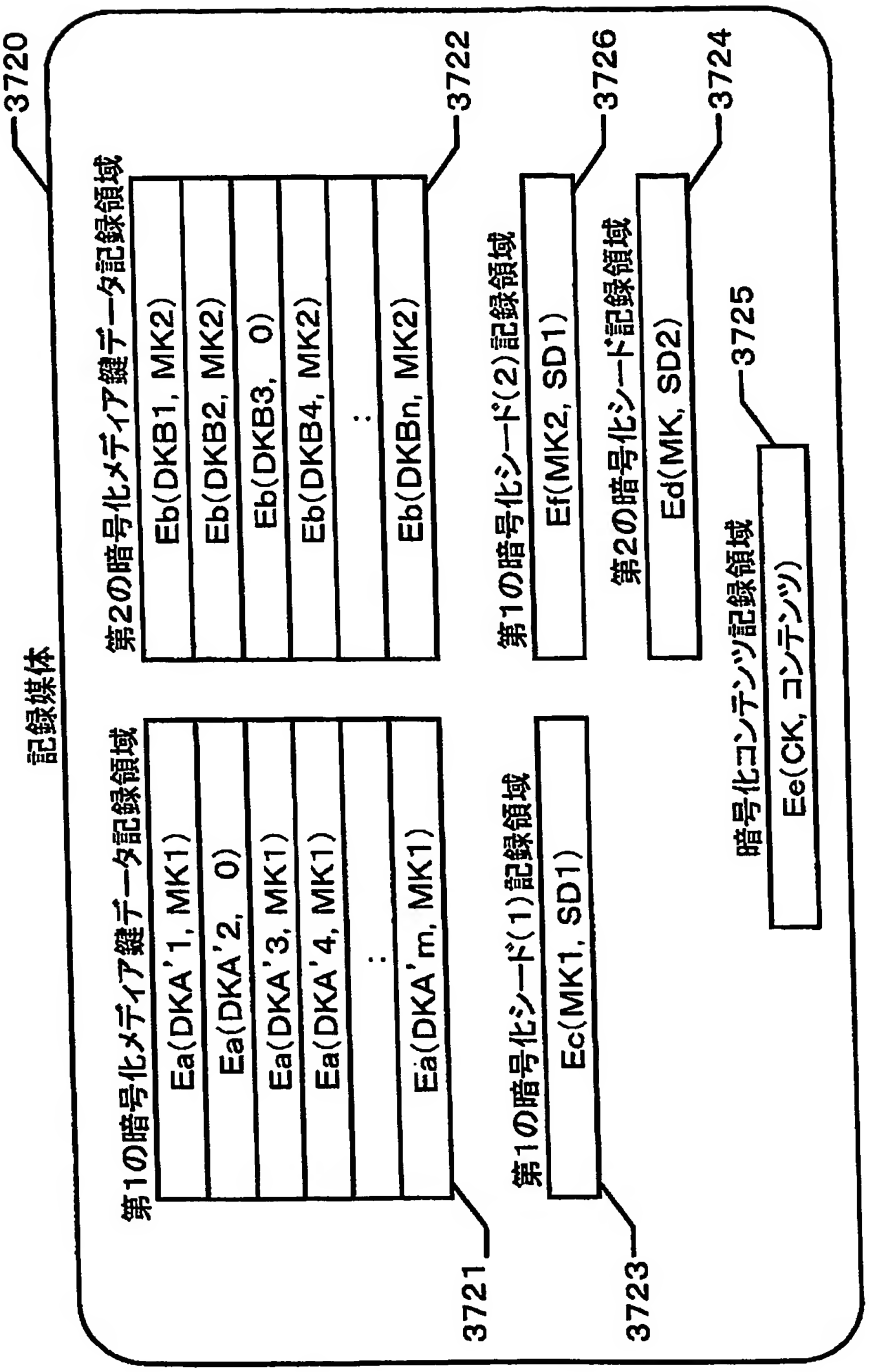
【図４０】

本発明の実施の形態7における記録媒体に記録するデータの具体例



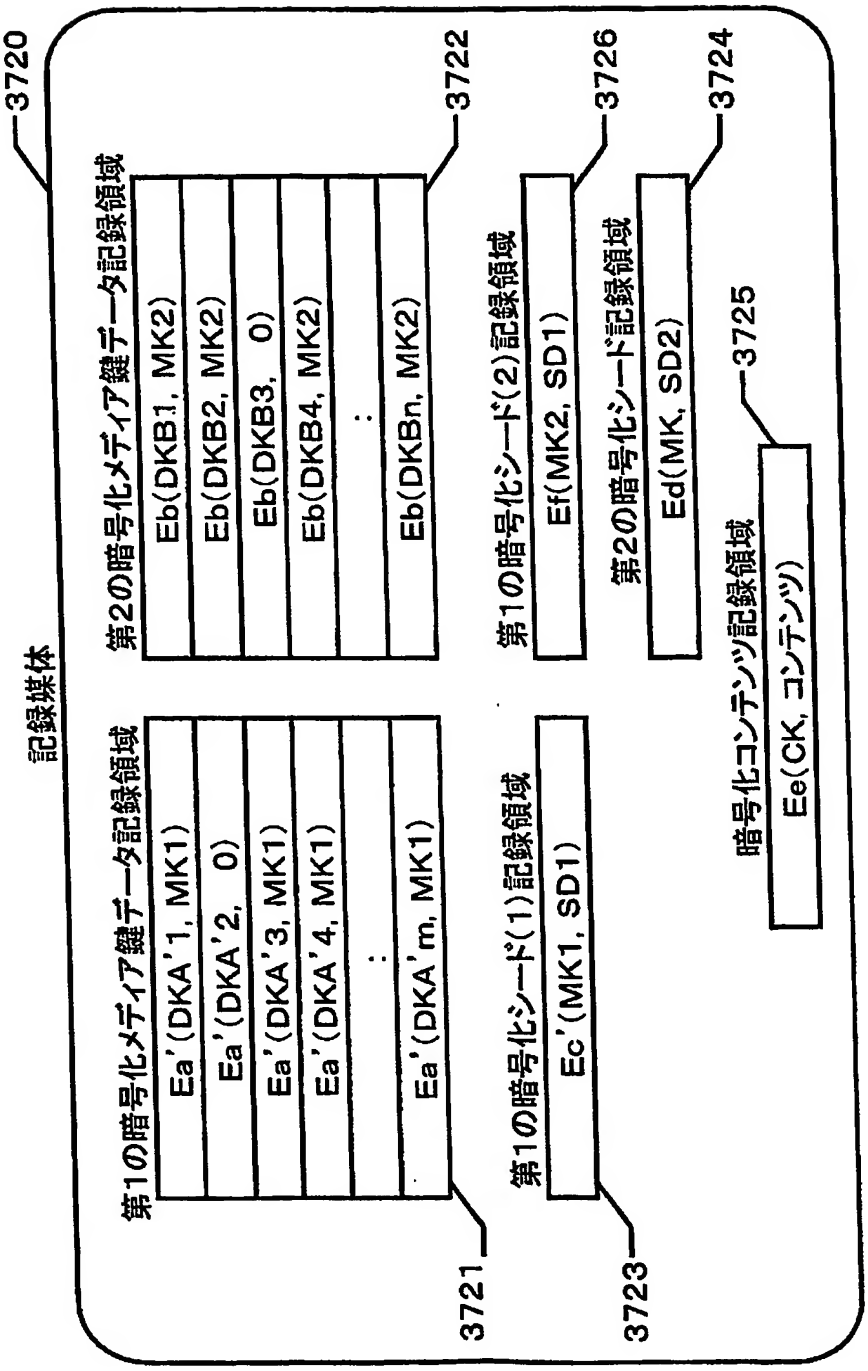
【図４１】

本発明の実施の形態7におけるシステム更新の具体例1



【図４２】

本発明の実施の形態7におけるシステム更新の具体例2



【書類名】要約書
【要約】
【課題】装置内に設けるメモリのサイズを小さくでき、かつ、あるカテゴリの装置が不正に解析されてアルゴリズムや多数の鍵が暴露された場合でも、他のカテゴリの装置に変更を加えることなくシステム全体の無効化機能を維持することのできる著作権保護システムを提供する。
【解決手段】装置は複数のカテゴリに分類されており、メディア鍵と各カテゴリに属する装置が保有するデバイス鍵データとから各カテゴリの特定の装置が保有するデバイス鍵を無効化するための無効化データを各カテゴリに対してそれぞれ生成し、記録媒体に記録する。
【選択図】図１

特願２００３－２８６６５７

出願人履歴情報

識別番号　［０００００５８２１］

１．変更年月日　１９９０年　８月２８日
［変更理由］　新規登録
住　所　大阪府門真市大字門真１００６番地
氏　名　松下電器産業株式会社